ESET
Remote Administrator 4
Manual de instalación y Guía del usuario

ESET Remote Administrator 4

Copyright © 2010 **de ESET, spol. s r.o.**
ESET Remote Administrator 4 ha sido desarrollado por ESET, spol. s r.o.
Para obtener más información, visite el sitio 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 la previa autorización por escrito del autor.
ESET, spol. s r.o. se reserva el derecho de modificar 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. 31.8.2010

Contenido

1. Introducción 5

1.1 Novedades 5

1.2 Arquitectura del programa 7

2. Instalación de ERA Server y ERA Console 8

2.1 Requisitos 8
2.1.1 Requisitos de software 8
2.1.2 Requisitos de rendimiento 8
2.1.3 Puertos utilizados 10

2.2 Guía de instalación básica 10
2.2.1 Información general del entorno (estructura de la red) 10
2.2.2 Antes de la instalación 11
2.2.3 Instalación 12
2.2.3.1 instalación del ERA Server 12
2.2.3.1.1 Instalación en clúster 13
2.2.3.2 instalación de la ERA Console 13
2.2.3.3 Mirror 13
2.2.3.4 Tipos de bases de datos compatibles con el ERA Server 14
2.2.3.4.1 Requisitos básicos 14
2.2.3.4.2 Configuración de la conexión de la base de datos 15
2.2.3.4.3 Instalación sobre una base de datos ya existente 16

2.3 Situación: instalación en un entorno empresarial 16
2.3.1 Información general del entorno (estructura de la red) 16
2.3.2 Instalación 17
2.3.2.1 Instalación en la sede 17
2.3.2.2 Sucursal: instalación del ERA Server 17
2.3.2.3 Sucursal: instalación del servidor Mirror HTTP 17
2.3.2.4 Sucursal: instalación remota en clientes 17
2.3.3 Otros requisitos para los entornos empresariales 18

3. Trabajo con ERAC 19

3.1 Conexión a ERAS 19

3.2 ERAC - Ventana principal 20

3.3 Filtrado de la información 21
3.3.1 Filtro 21
3.3.2 Menú contextual 22
3.3.3 Modo Vista 23

3.4 Fichas de ERAC 23
3.4.1 Descripción general de las fichas y los clientes 23
3.4.2 Replicación e información en fichas individuales 24
3.4.3 Ficha Clientes 25
3.4.4 Ficha Registro de amenazas 27
3.4.5 Ficha Registro del cortafuegos 28
3.4.6 Ficha Registro de sucesos 28
3.4.7 Ficha Registro de análisis 28
3.4.8 Ficha Registro móvil 29
3.4.9 Ficha Cuarentena 29
3.4.10 Ficha Tareas 29
3.4.11 Ficha Informes 30
3.4.12 Ficha Instalación remota 30

3.5 Configuración de la ERA Console 30
3.5.1 Ficha Conexión 30
3.5.2 Columnas - Ficha Mostrar u ocultar 30
3.5.3 Ficha Colores 30
3.5.4 Ficha Rutas 30
3.5.5 Ficha Fecha/Hora 30
3.5.6 Ficha Otras opciones 31

3.6 Modos de visualización 31

3.7 ESET Configuration Editor 32
3.7.1 Capa de configuración 32
3.7.2 Entradas de configuración clave 33

4. Instalación de las soluciones cliente de ESET 35

4.1 Instalación directa 35

4.2 Instalación remota 35
4.2.1 Requisitos 38
4.2.2 Configuración del entorno para la instalación remota 38
4.2.3 Instalación impulsada remota 39
4.2.4 Instalación remota por correo electrónico/inicio de sesión 42
4.2.5 Instalación remota personalizada 44
4.2.6 Actualizar 45
4.2.7 Cómo evitar instalaciones repetidas 45

4.3 Instalación en un entorno empresarial 46

5. Administración de ordenadores cliente 47

5.1 Tareas 47
5.1.1 Tarea de configuración 48
5.1.2 Tarea Análisis a petición 48
5.1.3 Tarea Actualizar ahora 49
5.1.4 Tarea Script de SysInspector 49
5.1.5 Tarea Restaurar/eliminar de la cuarentena 49
5.1.6 Tarea Generar registro de auditoría de seguridad 50
5.1.7 Tarea Mostrar notificación 50
5.1.8 Tarea interactiva 50

5.2 Administrador de grupos 51
5.2.1 Grupos estáticos 52
5.2.2 Grupos paramétricos 52
5.2.3 Sincronización de Active Directory 53

5.3 Directivas 54
5.3.1 Funcionamiento y principios básicos 54
5.3.2 Cómo crear directivas 54
5.3.3 Directivas virtuales 55
5.3.4 Función y objetivo de las directivas en la estructura de árbol de directivas 56
5.3.5 Visualización de directivas 57
5.3.6 Importación/exportación de directivas 57
5.3.7 Asignación de directivas a clientes 57
5.3.7.1 Directiva predeterminada para clientes principales 57
5.3.7.2 Asignación manual 58
5.3.7.3 Reglas de la directiva 58
5.3.8 Eliminación de directivas 59
5.3.9 Configuración especial 59
5.3.10 Situaciones de implementación de directivas 60
5.3.10.1 Cada servidor es una unidad independiente y las directivas se definen localmente 60

5.3.10.2 Los servidores se administran de forma individual y las directivas se gestionan localmente, pero la Directiva principal predeterminada se hereda del servidor superior ... 61
5.3.10.3 Herencia de directivas de un servidor superior ... 62
5.3.10.4 Asignación de directivas sólo desde el servidor superior ... 63
5.3.10.5 Uso de las reglas de la directiva ... 63
5.3.10.6 Uso de grupos ... 64
5.4 Notificaciones ... 64
5.4.1 Administrador de notificaciones ... 65
5.4.1.1 Notificaciones mediante captura del SNMP ... 70
5.4.2 Creación de reglas ... 70
5.5 Información detallada de los clientes ... 71
5.6 Cuarentena centralizada ... 72

6. Asistente de combinación de reglas del cortafuegos ... 73

7. Informes ... 74

7.1 Situación de creación de informe de ejemplo ... 76

8. Configuración del servidor de ESET Remote Administrator (ERAS) ... 77

8.1 Seguridad ... 77
8.2 Mantenimiento del servidor ... 77
8.3 Servidor Mirror ... 78
8.3.1 Funcionamiento del servidor Mirror ... 79
8.3.2 Tipos de actualizaciones ... 79
8.3.3 Cómo activar y configurar el Mirror ... 80
8.3.4 Mirror para clientes con NOD32 versión 2.x ... 82
8.4 Replicación ... 82
8.5 Registro ... 84
8.6 Administración de licencias ... 84
8.7 Configuración avanzada ... 85
8.8 Otras opciones ... 85

9. ESET Remote Administrator Maintenance Tool ... 87

9.1 Información del ERA Server ... 87
9.2 Tipo de tarea ... 87
9.2.1 Detener el ERA Server ... 87
9.2.2 Iniciar el ERA Server ... 87
9.2.3 Transferencia de la base de datos ... 87
9.2.4 Copia de seguridad de la base de datos ... 88
9.2.5 Restauración de la base de datos ... 88
9.2.6 Eliminar tablas ... 88
9.2.7 Instalación de una clave de licencia nueva ... 88
9.2.8 Modificación de la configuración del servidor ... 88

10. Resolución de problemas ... 89

10.1 Preguntas frecuentes ... 89
10.1.1 Problemas con la instalación de ESET Remote Administrator en un servidor Windows 2000/2003 ... 89
10.1.2 ¿Qué significa el código de error GLE? ... 89
10.2 Códigos de error que aparecen con frecuencia ... 89
10.2.1 Mensajes de error generados al utilizar ESET Remote Administrator para instalar ESET Smart Security o ESET NOD32 Antivirus de forma remota ... 89
10.2.2 Códigos de error que aparecen con frecuencia en el registro era.log ... 90
10.3 ¿Cómo diagnosticar problemas con ERAS? ... 91

11. Ayudas y sugerencias ... 92

11.1 Programador de Tareas ... 92
11.2 Eliminación de perfiles existentes ... 94
11.3 Exportación y otras características de la configuración XML del cliente ... 95
11.4 Actualización combinada para portátiles ... 95
11.5 Instalación de productos de terceros con ERA ... 97

12. ESET SysInspector ... 98

12.1 Introducción a ESET SysInspector ... 98
12.1.1 Inicio de ESET SysInspector ... 98
12.2 Interfaz de usuario y uso de la aplicación ... 98
12.2.1 Controles de programa ... 99
12.2.2 Navegación por ESET SysInspector ... 100
12.2.3 Comparar ... 101
12.3 Parámetros de la línea de comandos ... 102
12.4 Script de servicio ... 102
12.4.1 Generación de scripts de servicio ... 103
12.4.2 Estructura del script de servicio ... 103
12.4.3 Ejecución de scripts de servicio ... 105
12.5 Accesos directos ... 106
12.6 Requisitos del sistema ... 107
12.7 Preguntas frecuentes ... 107

13. ESET SysRescue ... 109

13.1 Requisitos mínimos ... 109
13.2 Cómo crear un CD de recuperación ... 109
13.2.1 Carpetas ... 109
13.2.2 ESET Antivirus ... 110
13.2.3 Configuración avanzada ... 110
13.2.4 Dispositivo USB de arranque ... 110
13.2.5 Grabar ... 110
13.3 Trabajo con ESET SysRescue ... 111
13.3.1 Uso de ESET SysRescue ... 111

1. Introducción

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

ESET Remote Administrator no proporciona por sí mismo ninguna forma de protección frente a código malicioso. ERA depende de la presencia de una solución de seguridad ESET en estaciones de trabajo o servidores, como ESET NOD32 Antivirus o ESET Smart Security.
Para realizar la implementación completa de un conjunto de soluciones de seguridad ESET, efectúe los pasos siguientes:

- Instalación del ERA Server (ERAS),
- Instalación de la ERA Console (ERAC),
- Instalación en ordenadores cliente (ESET NOD32 Antivirus, ESET Smart Security, Linux ESET Security cliente, 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:\Archivos de programa*
%ALLUSERSPROFILE% = normalmente, *C:\Documents and Settings\All Users*

1.1 Novedades

ESET Remote Administrator Versión 4.0

- Compatibilidad con ESET Smart Security/ESET NOD32 Antivirus 4.2
- Compatibilidad con ESET Mail Security 4 for Microsoft Exchange Server
- Compatibilidad con la solución de seguridad para ordenadores de sobremesa Linux/Mac (ESET NOD32 Antivirus 4)
- Compatibilidad con ESET Mobile Security

Nuevas características
- Instalación remota: diseño nuevo
- Administración de grupos: diseño nuevo (grupos estáticos, grupos paramétricos, sincronización mejorada de Active Directory)
- Filtro: funcionalidad mejorada (filtros de directiva, filtros de grupos estáticos y paramétricos)
- Directivas: nuevos parámetros para las reglas de política (compatibilidad con grupos paramétricos), importación/exportación de directivas y reglas de directiva, combinación de tareas del programador de tareas, asistente de reglas de directiva
- Notificaciones: compatibilidad con grupos paramétricos y varias mejoras menores
- Vista centralizada de la cuarentena de clientes (para clientes de ESS/EAV versión 4 o superior)
- Informes: compatible con grupos estáticos y paramétricos, nuevos tipos de informes (registro móvil, cuarentena, cortafuegos), nuevas plantillas
- Asistente de combinación de reglas del cortafuegos: asistente para la combinación de reglas creadas en el modo de aprendizaje
- Autenticación de dominio de Windows para el usuario de la ERA Console
- Compatibilidad con clústeres pasivos de Windows
- Permite la reinstalación de versiones anteriores de ERA (3.x, 2.x, 1.x) y la migración de datos
- Cifrado de comunicación con AES-256

Nuevo ESET Configuration Editor
- Compatibilidad con los productos de seguridad de ESET
- Compatibilidad con las características nuevas del ERA Server
- Archivos de licencia comprimidos
- Posibilidad de agregar tareas programadas predefinidas

ESET Remote Administrator Versión 3.0

- Compatibilidad con los productos de seguridad de ESET 4.x
- Compatibilidad con soluciones de Linux

Nuevas características
- Administración de directivas
- Administrador de notificaciones
- Acceso de sólo lectura a la consola
- Compatibilidad con ESET SysInspector
- Escalabilidad de la transferencia de datos mejorada
- Eliminación de clientes replicados
- Combinación de claves de licencia/Administrador de licencias
- Mirror para ESET NOD32 Antivirus 2.x
- Nueva configuración
- Opción de filtrado basado en dominios añadida a Buscar ordenadores no registrados
- Compresión de los registros de servidor (zip)
- Solución de problemas menores y adición de varias características secundarias
- CD de recuperación

Mejoras en el servidor interno
- Compatibilidad con otras bases de datos (MS Access, MS SQL Server, Oracle y MySQL)

Nuevo ESET Configuration Editor
- Compatibilidad con los productos de seguridad de ESET 4.x

ESET Remote Administrator Versión 2.0

- Compatibilidad con los nuevos productos de seguridad de ESET versión 3 (ESET Smart Security, ESET NOD32 Antivirus)
- Nuevos registros (nuevas columnas, registros del cortafuegos personal de ESET)
- Nueva información de estado de cliente para los clientes de la versión 3 (Estado de la protección, Características de protección, Información del sistema)
- Tareas (configuración, actualizar ahora, análisis a petición, tarea interactiva)
- Sigue siendo compatible con productos NOD32 versión 2

Nuevas características
- Identificación del cliente ampliada (se ha agregado la dirección MAC)
- Instalación remota ampliada (compatible con paquetes .msi y personalizados)
- Mejoras de seguridad (posibilidad de cifrado para todos los clientes de servidor nuevos)
- Mejoras del rendimiento (compresión en el protocolo de comunicación)
- Función de reenvío de datos de ThreatSense.Net añadida a través de ERA Server
- Mejoras en la interfaz gráfica de usuario (nuevos gráficos, colores de estado mejorados, filtros ampliados, cuadros de diálogo ajustables)
- Nueva plantilla de informes (Tema ESS)
- Control del rendimiento del servidor (datos, consultas)
- Funcionalidad de actualización en el ERA Server (permite actualizar información importante)
- Funcionalidad de mirror en el ERA Server
- Instalación remota ampliada (compatible con paquetes .msi y personalizados, posibilidad de instalación remota de ERA, diagnóstico)

Mejoras en el servidor interno
- Nueva replicación (prioridad de replicación, mejor replicación en varios niveles)
- Nueva estructura de la base de datos
- Nueva estructura del directorio
- Mejoras de seguridad interna

Nuevo ESET Configuration Editor
- Compatible con productos de seguridad de ESET versión 2 y 3
- Posibilidad de configurar el ERA Server
- Otras características secundarias nuevas (búsqueda, configuración personalizada)

Nuevo instalador (MSI)
- Migración de la base de datos desde versiones anteriores

Nueva documentación (ayuda, manual)

1.2 Arquitectura del programa

Técnicamente, ESET Remote Administrator consta de dos componentes individuales: ERA Server (ERAS) y ERA Console (ERAC). Puede ejecutar un número ilimitado de consolas y ERA Server en la red, ya que no existen limitaciones de uso en el acuerdo de licencia. La única limitación es el número total de clientes que puede administrar la instalación de ERA.

ERA Server (ERAS)

El componente de servidor de ERA se ejecuta como un servicio dentro de los siguientes sistemas operativos basados en Microsoft Windows® NT: NT4 SP6, 2000, XP, 2003, Vista, 7 y 2008. La principal tarea de este servicio consiste en recoger información de los clientes y enviarles distintas solicitudes. Estas solicitudes, que incluyen tareas de configuración, solicitudes de instalación remota, etc., se crean mediante la ERA Console (ERAC). ERAS es un punto de encuentro entre ERAC y los ordenadores cliente, un lugar donde se procesa, mantiene o modifica toda la información antes de su transferencia a los clientes o a ERAC.

ERA Console (ERAC)

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

%ProgramFiles%\ESET\ESET Remote Administrator\Console

Cuando instale ERAC, es posible que tenga que indicar el nombre de ERAS. Tras el inicio, la consola se conectará automáticamente a este servidor. ERAC también se puede configurar tras la instalación.

2. Instalación de ERA Server y ERA Console

2.1 Requisitos

ERAS funciona como un servicio, por lo que requiere un sistema operativo basado en Microsoft Windows NT (NT4 SP6, 2000, XP, 2003, Vista, 7 o 2008). ERAS no necesita Microsoft Windows Server Edition para funcionar; no obstante, es recomendable instalar ERAS en sistemas operativos basados en servidor para conseguir un funcionamiento perfecto. Un ordenador con ERAS instalado debe estar en línea siempre y ser accesible a través de la red de ordenador mediante:

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

NOTA: ESET Remote Administrator 4 es totalmente compatible con versiones anteriores (3.x, 2.x, 1.x) y la migración de datos.

2.1.1 Requisitos de software

ERA Server

Sistemas operativos de 32 bits:	Windows NT4 SP6 y versiones posteriores
Sistemas operativos de 64 bits:	Windows XP y versiones posteriores
Bases de datos:	Microsoft Access (integrado) Microsoft SQL Server 2005 y versiones posteriores MySQL 5.0 y versiones posteriores ORACLE 9i y versiones posteriores
Windows Installer:	2.0

ERA Console

Sistemas operativos de 32 bits:	Windows 2000 y versiones posteriores
Sistemas operativos de 64 bits:	Windows XP y versiones posteriores
Windows Installer:	2.0
Internet Explorer:	se recomienda la versión 6.0, la versión mínima es 4.0 (puede que algunos informes no se muestren correctamente)

2.1.2 Requisitos de rendimiento

El rendimiento del servidor puede variar en función de los parámetros siguientes:

1. **Base de datos utilizada**
   - Base de datos de MS Access: está instalada en el servidor de forma predeterminada. Recomendamos utilizar esta solución cuando se presta servicio a muchos clientes. Esta base de datos tiene un límite de tamaño de 2 GB. Por este motivo, debe activar las limpiezas en el servidor y definir un intervalo (en **Herramientas** > **Opciones del servidor** > **Mantenimiento del servidor**) para eliminar los datos antiguos.
   - Otras base de datos (MySQL, MSSQL, ORACLE) requieren una instalación independiente, pero pueden ofrecer un mejor rendimiento del servidor. Es vital utilizar un hardware adecuado para cada motor de bases de datos (especialmente ORACLE), de conformidad con las recomendaciones técnicas del distribuidor.
   - Si selecciona ORACLE como solución de base de datos, debe establecer el número de cursores en un valor superior al valor de **Número máximo de conexiones activas** (en **Herramientas** > **Opciones del servidor** > **Avanzadas** > **Modificar configuración avanzada** > **Avanzadas**; el valor predeterminado es 500). El número final de cursores debe tener en cuenta el número de servidores inferiores (si se utiliza la replicación) y los cursores que utilizan otras aplicaciones que acceden al motor de base de datos.
   - Normalmente, el rendimiento del servidor es mayor cuando se utilizan base de datos externas (es decir, instaladas en una máquina física diferente).

2. **Intervalo de conexión de clientes**
   - El intervalo de conexión de clientes está establecido en 10 minutos, de forma predeterminada, en ESET Smart Security/ESET NOD32 Antivirus versión 4.2 o posterior. Si necesita actualizar el estado del cliente con más o

menos frecuencia, puede cambiar este ajuste. Recuerde que un intervalo de conexión de clientes más corto afectará al rendimiento del servidor.

3. **Promedio de sucesos que notifican los clientes por conexión**
   - Toda la información enviada desde el cliente al servidor se indica en el suceso en cuestión (por ejemplo, registro de amenazas, registro de sucesos, registro de análisis, cambio de configuración, etc.). Este parámetro no se puede cambiar directamente, pero se puede alterar al modificar otros ajustes relacionados. Por ejemplo, en la configuración avanzada del servidor (en **Herramientas** > **Opciones del servidor** > **Mantenimiento del servidor**), se puede establecer el número máximo de registro que acepta el servidor (este ajuste incluye a los clientes que se pueden conectar directamente y a los clientes replicados). Durante el funcionamiento normal, el promedio a largo plazo es aproximadamente de 1 suceso cada 4 horas por cliente.

4. **Hardware y sistema operativo utilizados**
   - Recomendamos encarecidamente el uso del hardware mínimo indicado para el sistema operativo del servidor, teniendo en cuenta el número de clientes a los que se presta servicio.

Sobrecarga
Cuando están sobrecargados (p. ej., se conectan 20.000 clientes a un servidor que sólo tiene capacidad para atender a 10.000 clientes cada 10 minutos), los servidores omiten algunos de los clientes conectados. Normalmente, los servidores atienden clientes alternos (uno sí y otro no), como si el intervalo de conexión de clientes estuviese establecido en 20 minutos, en lugar de 10 minutos. Las denegaciones de servicio se registran de la manera siguiente: "*<SERVERMGR_WARNING> ServerThread: se ha alcanzado el número máximo de procesos para conexiones activas (500), el servidor omitirá esta conexión*". También pueden producirse denegaciones de servicio durante las sobrecargas temporales del servidor.
El valor se puede cambiar en **Número máximo de conexiones activas** (el valor predeterminado es 500), en la configuración avanzada del servidor, aunque es recomendable hacerlo únicamente en casos excepcionales (p. ej., para resolver problemas específicos). En caso de que hubiese un exceso de recursos del sistema y rendimiento del motor de base de datos, puede utilizar esta configuración para ajustar el rendimiento general del servidor.

Transferencia de datos a través de una red
Durante el funcionamiento normal de un servidor, se calcula que un cliente que se conecte cada 10 minutos informará de 0,04 sucesos por conexión, es decir, un suceso cada 4 horas por cliente. Esta actividad producirá aproximadamente 2 kilobytes de tráfico por conexión.
En el caso de un brote de virus, si un cliente informa de 7 sucesos cada vez que se conecta, el tráfico podría aumentar a 240 kilobytes por conexión. Si utiliza la compresión (predeterminado), los datos transferidos tendrían un tamaño alrededor de un 50% menor, es decir, de 120 kilobytes por conexión.
Los datos incluyen las conexiones directas de clientes; las conexiones replicadas no se tienen en cuenta. La replicación se produce con una frecuencia mucho menor y sirve para enviar sucesos nuevos desde servidores inferiores. Los sucesos que se replicarán automáticamente, y su nivel de detalle, se pueden configurar en la configuración avanzada del servidor (en **Herramientas** > **Opciones del servidor** > **Avanzadas** > **Modificar configuración avanzada** > **Replicación**). En la sección Mantenimiento del servidor, puede configurar el nivel máximo de los registros que aceptará el servidor superior. Este ajuste se aplica tanto a los clientes que se conectan directamente como a los clientes replicados.

Requisitos de capacidad de almacenamiento
La instalación limpia del producto con una base de datos de MS Access ocupa hasta 60 MB de espacio en disco.
La mayor parte del espacio de almacenamiento lo ocupan los sucesos de cliente, que se almacenan en la base de datos y en un repositorio del disco (el directorio predeterminado es *C:\Documents and Settings\All Users\Application Data\Eset\ESET Remote Administrator\Server*). ERA requiere como mínimo un 5% de espacio libre en disco. Si se supera este mínimo, el servidor dejará de recibir algunos sucesos de cliente. Este ajuste está disponible en **Herramientas** > **Opciones del servidor** > **Avanzadas** > **Modificar configuración avanzada** > **Avanzadas** > **Uso máx. de espacio en disco**. La operación normal con la configuración de desinfección predeterminada (eliminación de sucesos con más de 3 meses) requiere aproximadamente 10 GB de espacio libre en disco por cada 1.000 clientes.

Caso práctico

Un servidor que utilice una base de datos de MS Access cuyos clientes se conecten cada 5 minutos e informen de una media de 7 sucesos (p. ej., registro de amenazas, registro de sucesos, registro de análisis, cambio de configuración, etc.) por conexión pueden atender temporalmente hasta 3.000 clientes. Esta situación representa un estado de sobrecarga temporal, como informar durante un brote de virus, etc.
Si el servidor utiliza una base de datos MySQL externa y el intervalo de conexión de clientes está establecido en 10 minutos (con una generación de 0,02 sucesos por conexión), el número máximo de clientes que puede atender el servidor ascenderá a 30.000. Esta situación muestra un rendimiento óptimo de la base de datos, en el que los clientes

informan de un número relativamente pequeño de sucesos.
Durante la operación normal, con una base de datos de MS Access y un intervalo de conexión de clientes de 10 minutos, el servidor podrá atender a un máximo de 10.000 clientes.

2.1.3 Puertos utilizados

En la tabla siguiente se indican las posibles comunicaciones de red con ERAS instalado. El proceso EHttpSrv.exe está a la escucha en el puerto TCP 2221 y el proceso era.exe, en los puertos TCP 2222, 2223, 2224 y 2846. El resto de las comunicaciones utilizan procesos nativos del sistema operativo (por ejemplo, "NetBIOS sobre TCP/IP").

Protocolo	Puerto	Descripción
TCP	2221 (escucha de ERAS)	Puerto predeterminado que utiliza la característica Mirror integrada en ERAS (versión HTTP).
TCP	2222 (escucha de ERAS)	Comunicación entre clientes y ERAS.
TCP	2223 (escucha de ERAS)	Comunicación entre ERAC y ERAS

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

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

Los puertos predeterminados 2221, 2222, 2223, 2224 y 2846 se pueden cambiar si hay otras aplicaciones que los están utilizando.

Para cambiar los puertos predeterminados que utiliza ERA, haga clic en **Herramientas** > **Opciones del servidor...** Para cambiar el 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 **Avanzadas**.

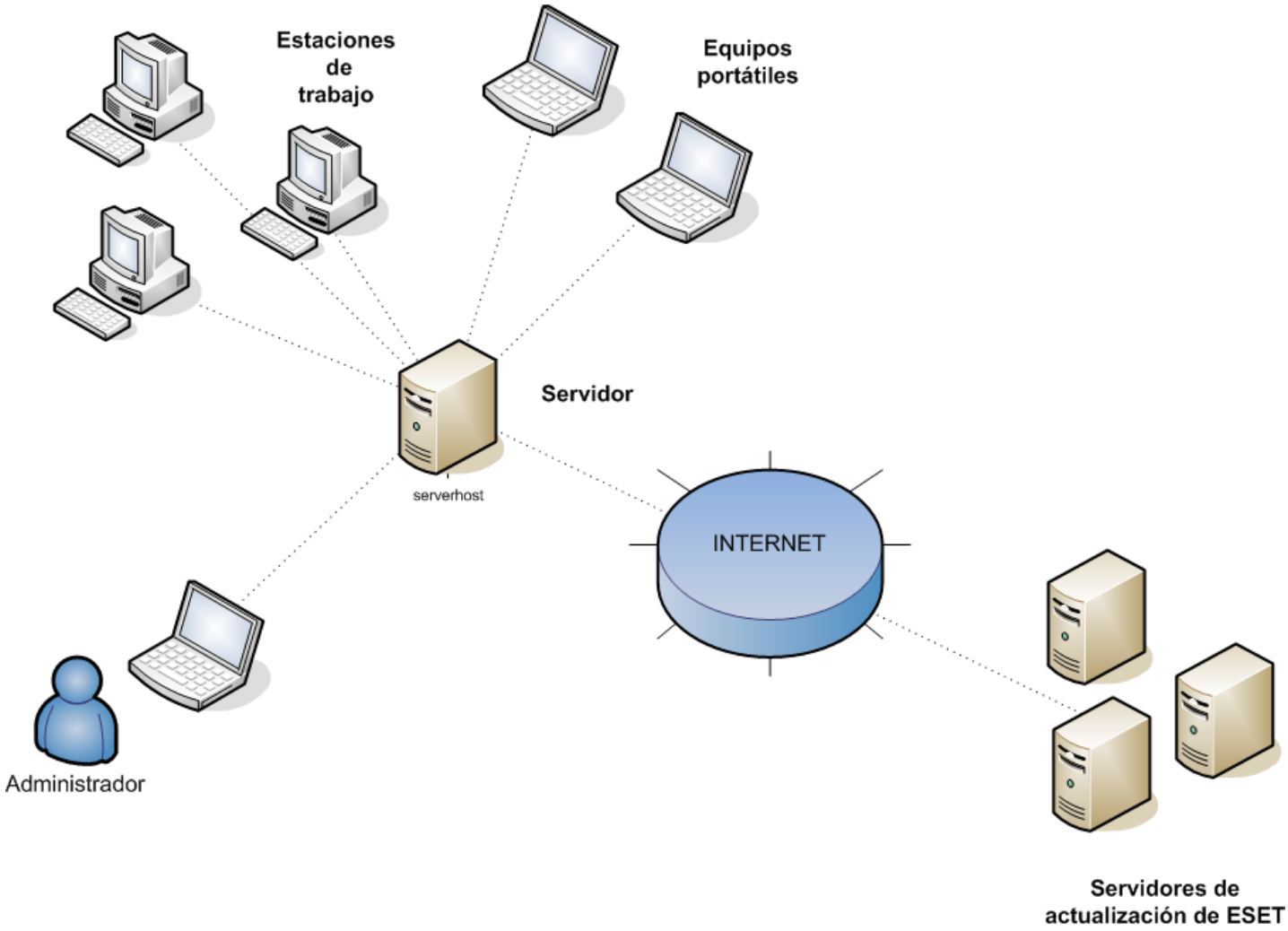
Los puertos predeterminados 2222, 2223, 2224 y 2846 también se pueden modificar durante el modo de instalación avanzada (ERAS).

2.2 Guía de instalación básica

2.2.1 Información general del entorno (estructura de la red)

Por lo general, una red empresarial consta de una red de área local (LAN), por lo que se aconseja la instalación de ERAS y de un servidor Mirror. El servidor Mirror se puede crear en 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/7, conectados por red en 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 de 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 podría parecerse a la que se muestra a continuación:



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.x
ESET Smart Security 3.x
ESET NOD32 Antivirus 4.x
ESET NOD32 Antivirus 3.x
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 ERA Server

Instale ERAS en el servidor GHOST (consulte el ejemplo de Información general del entorno 10). 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 o .zip que hace posible el funcionamiento de ERAS durante el período estipulado en la licencia). A continuación, el programa le pedirá que establezca unos parámetros de actualización (nombre de usuario, contraseña y servidor de actualización). También 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 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 ordenador. Esta es la información más importante para llevar a cabo la instalación remota. Si no se especifica un nombre durante la instalación, el instalador proporcionará automáticamente el valor de la variable de sistema %COMPUTERNAME%, que es suficiente en la mayoría de los casos. También es importante seleccionar la base de datos adecuada en la que debe almacenarse la información de ERAS. Consulte el capítulo Tipos de bases de datos compatibles con el ERA Server 14 para obtener más información.

Importante: las versiones recientes de Microsoft Windows (Windows Vista, Windows Server 2008 y Windows 7) aplican directivas de seguridad que limitan los permisos de las cuentas de usuario local, por lo que es posible que el usuario no pueda ejecutar operaciones de red específicas. Si el servicio de ERA se ejecuta en una cuenta de usuario local, es posible que se produzcan problemas de instalación impulsada en determinadas configuraciones de red (p. ej., durante la instalación remota desde un dominio en un grupo de trabajo). Si se utiliza Windows Vista, Windows Server 2008 o Windows 7, es recomendable ejecutar el servicio de ERA en cuentas con suficientes derechos de red. Puede especificar la cuenta de usuario donde desea ejecutar ERA en la situación de instalación Avanzada.

Nota: Aunque ERA Server tiene compatibilidad Unicode completa, hay casos en los que el servidor convierte algunos caracteres a ANSI o viceversa (p. ej.: email, computername). En estas situaciones, se usa el idioma para la configuración de los programas que no son unicode. Le recomendamos que cambie esta configuración para que coincida con el entorno del servidor local, incluso si no está utilizando una versión localizada de ERA (p. ej., si utiliza una variedad de la lengua inglesa). Puede encontrar esta configuración en **Panel de control** > **Configuración regional y de idioma**en la pestaña **Opciones avanzadas**.

Los componentes del programa de ERAS se instalan, de manera predeterminada, 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

El servicio de ERAS se inicia automáticamente tras la instalación. La actividad de ERAS queda registrada en esta ubicación:

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

Instalación de la línea de comandos

ERAS se puede instalar con los siguientes parámetros de la línea de comandos:

/q: instalación silenciosa. El usuario no puede intervenir en ningún momento. No se muestra ninguna ventana de diálogo.
/qb: el usuario no puede intervenir en ningún momento, pero el proceso de instalación se indica mediante una barra de progreso.

Ejemplo: *era_server_nt32_ENU.msi /qb*

Los parámetros y la configuración de la instalación de la línea de comandos se pueden complementar con el archivo de configuración *.xml* (*cfg.xml*) del administrador, que debe estar en la misma carpeta que el archivo de instalación *.msi* de

ERA. El archivo de configuración se puede crear en ESET Configuration Editor y le permite configurar varios ajustes de ERA. Consulte el capítulo ESET Configuration Editor 32 para obtener más detalles.

2.2.3.1.1 Instalación en clúster

La situación de instalación avanzada también le permite activar la **Instalación en clúster**. Si la instalación en clúster está activada, tendrá que especificar la ruta de acceso a una carpeta de datos compartidos del clúster que sea totalmente accesible para todos los demás nodos del clúster (es decir, debe tener permisos de lectura y escritura para esta carpeta). Puede tratarse de un disco de quórum o una carpeta compartida con formato UNC. Si se utiliza una carpeta compartida, es necesario activar el uso compartido para **Ordenadores** en las propiedades de la carpeta compartida. Después, debe agregar el nombre de nodo del clúster a **Permisos de los recursos compartidos** con todos los derechos. Debe instalar el ERA Server individualmente en todos los nodos del clúster. Si no se utiliza la base de datos integrada de MS Access, es importante asegurarse de que todos los nodos del ERA Server se conectan a la misma base de datos. En los próximos pasos, también es importante establecer el nombre del nodo de clúster donde debe instalarse ERA como nombre del servidor.

Importante: es necesario configurar el servicio de ESET Remote Administrator Server (ERA_SERVER) como servicio genérico del clúster en la consola del Administrador de clústeres.

Si tiene previsto desinstalar el ERA Server, debe desactivar el nodo de clúster antes de hacerlo.

2.2.3.2 instalación de la ERA Console

Instale ESET Remote Administrator Console en el ordenador o portátil del administrador. Al final del modo de instalación Avanzada, escriba el nombre del ERA Server (o su dirección IP) al que debe conectarse automáticamente ERAC cuando se inicie. En nuestro ejemplo, el nombre del servidor es GHOST.

Tras la instalación, inicie ERAC y compruebe la conexión a ERAS. No se requiere ninguna contraseña de forma predeterminada para conectarse a un ERA Server (el campo de texto de la contraseña está vacío), pero se recomienda encarecidamente establecer una. Para crear una contraseña para la conexión a un ERA Server, haga clic en **Archivo** > **Cambiar contraseña...** y, a continuación, modificar la contraseña de 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 de ERAS, no modificarlo).

2.2.3.3 Mirror

Puede usar la ERA Console para activar el servidor de actualización de LAN (el Mirror del ERA Server). Después, este servidor se puede utilizar para actualizar las estaciones de trabajo situadas en la red local. Al activar el Mirror, se reduce el volumen de datos que se transfiere a través de la conexión a Internet.

Siga estos pasos:

1) Conecte la ERA Console al ERA Server; para ello, haga clic en **Archivo** > **Conectar**.
2) Desde la ERA Console, haga clic en **Herramientas** > **Opciones del servidor...** y, a continuación, en la ficha **Actualizaciones**.
3) En el menú desplegable **Servidor de actualización**, seleccione **Seleccionar automáticamente** y deje el valor de 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 mirror de actualización**. Conserve la ruta predeterminada para los archivos replicados y el puerto del servidor HTTP (2221). Deje **Autenticación** con el valor NINGUNA.
5) Haga clic en la ficha **Avanzadas** y en **Modificar configuración avanzada...** En el árbol de configuración avanzada, vaya a **ERA Server** > **Configuración** > **Mirror** > **Crear mirror 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 Mirror.

Para conocer más detalladamente las opciones de configuración del Mirror, consulte el capítulo Cómo activar y configurar el Mirror 80.

2.2.3.4 Tipos de bases de datos compatibles con el ERA Server

El programa usa de forma predeterminada el motor de Microsoft Access (base de datos Jet). ERAS 4.0 también es compatible con las siguientes bases de datos:

- Microsoft SQL Server 2005 y versiones posteriores
- MySQL 5.0 y versiones posteriores
- Oracle 9i y versiones posteriores

El tipo de base de datos se puede seleccionar durante el modo de instalación Avanzada de ERAS. Después de la instalación, el tipo de base de datos no se puede cambiar directamente desde ERA; pero sí se puede hacer con ERA Maintenance Tool 87.

NOTA:
- las bases de datos de Microsoft Access no son compatibles con Windows Server 2008 Core.
- SQL Server Express tiene límite de tamaño de la base de datos de 4 GB.

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 de ERAS puede crear una base de datos MySQL vacía, que recibe automáticamente 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 script**. Asegúrese de que la opción **Crear tablas en la nueva base de datos automáticamente** no está seleccionada.

Configuración de intercalación

La clasificación se lleva a cabo según los parámetros predeterminados de cada base de datos. Es necesario activar la no distinción entre mayúsculas y minúscula (CI).

Para activarla:

- Para MS SQL y MySQL, es necesario configurar un COLLATE con la opción CI activada.
- Para ORACLE, debe configurar un NLS_SORT con la opción CI activada.
- Para MS Access, no es necesario realizar ninguna acción, puesto que la opción CI ya está activada.

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 todos los clientes se conectan al mismo servidor, puede usar el juego de caracteres para el servidor ERA que desea instalar.

MARS (Multiple Active Result Sets, conjuntos de resultados activos múltiples)

Si se utiliza una base de datos MS SQL, es necesario un controlador OBDC compatible con MARS para un funcionamiento adecuado. De lo contrario, el servidor tendrá un comportamiento menos eficaz y registrará un mensaje de error similar al siguiente en el registro del servidor:

Database connection problem. It is strongly recommended to use odbc driver that supports multiple active result sets (MARS). The server will continue to run but the database communication may be slower. See the documentation or contact ESET support for more information.

Si el problema se produce con una base de datos que no sea MS SQL, el servidor registrará un mensaje similar al siguiente en el registro y se detendrá:

Database connection problem. Updating the odbc driver may help. You can also contact ESET support for more information.

Controladores no compatibles con MARS:
- SQLSRV32.DLL (2000.85.1117.00).
- SQLSRV32.DLL (6.0.6001.18000): nativo en Windows Vista y Windows Server 2008.

Controlador nativo compatible con MARS:
- SQLNCLI.DLL (2005.90.1399.00).

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 OBCD
   (haga clic **Inicio > Ejecutar** y escriba *odbcad32.exe*).

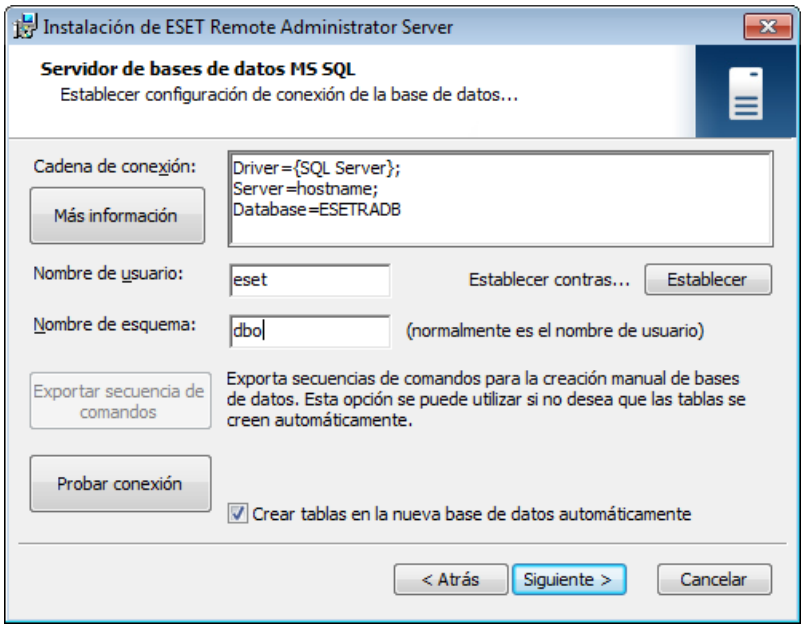
   Ejemplo de conexión de un DSN:
   DSN =ERASqlServer

   Importante: se recomienda el uso del *DSN del sistema* para que ERA funcione correctamente.

   Para realizar correctamente la instalación en MSSQL con autenticación de dominio de Windows, asegúrese de usar formato DSN al introducir la cadena de conexión.

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 de MS SQL Server:
   Controlador={SQL Server}; Servidor=nombre de host; Base de datos=ESETRADB



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 **Contraseña** de la conexión (con el botón **Establecer**). Las bases de datos Oracle y MS SQL Server también necesitan un **Nombre de esquema** (para MS SQL Server, suele ser igual al nombre de usuario).
Haga clic en **Probar conexión** para comprobar la conexión con el servidor de bases de datos.

Nota Es recomendable usar la autenticación de servidor de bases de datos en lugar de la autenticación de dominio de Windows.

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** (***Alerta:*** este comando elimina el contenido de las tablas y sobrescribe la estructura). Seleccione **Ignorar** para dejar las tablas intactas.

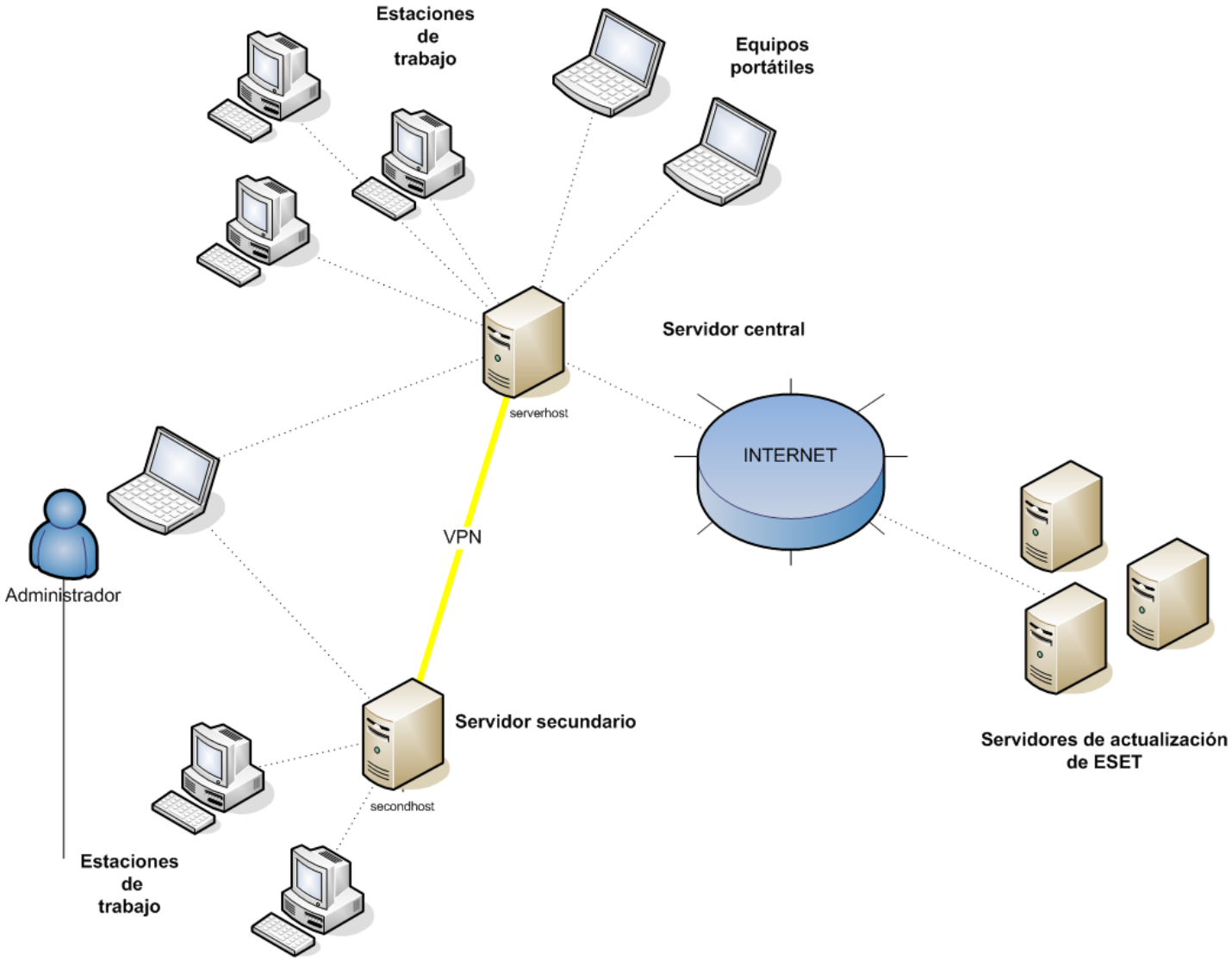
NOTA: si selecciona **Ignorar**, podrían aparecer errores de incoherencia en las bases de datos, especialmente si las tablas están dañadas o no son compatibles con la versión actual.

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

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 un servidor llamado LITTLE. Supongamos que existe un canal VPN lento entre la sede y la sucursal. En este caso, el servidor Mirror debería instalarse en el servidor LITTLE. También instalaremos un segundo ERA Server en LITTLE para crear un entorno más intuitivo y minimizar el volumen de datos transferidos.

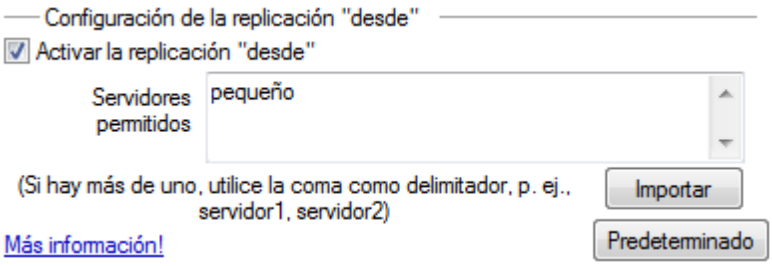


2.3.2 Instalación

2.3.2.1 Instalación en la sede

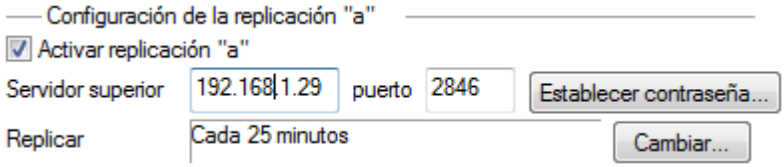
Las instalaciones de ERAS, ERAC y estaciones de trabajo cliente son muy similares a los casos anteriores. La única diferencia radica en la configuración de servidor ERAS maestro (GHOST). En **Herramientas** > **Opciones del servidor...** > **Replicación**, active la casilla de verificación **Activar replicación "desde"** y especifique 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**), utilice esta contraseña para la autenticación desde el servidor inferior.



2.3.2.2 Sucursal: instalación del ERA Server

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



2.3.2.3 Sucursal: instalación del servidor Mirror HTTP

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

Tal como se muestra en la figura del capítulo Información general del entorno 16, las actualizaciones de la sucursal no se descargan desde los servidores de actualización de ESET, sino del servidor de la sede (GHOST). El origen de de actualización se define mediante 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 autenticación.

Para obtener más información sobre la configuración del Mirror en ERAS, consulte el capítulo Servidor Mirror 78.

2.3.2.4 Sucursal: instalación remota en clientes

Una vez más, se puede utilizar el modelo anterior, con la diferencia de que es adecuado para todas las operaciones con ERAC conectada directamente al servidor ERAS de la sucursal (en nuestro ejemplo: LITTLE). Esto se hace para evitar que los paquetes de instalación se transfieran a través del canal VPN, lo que supone un proceso más lento.

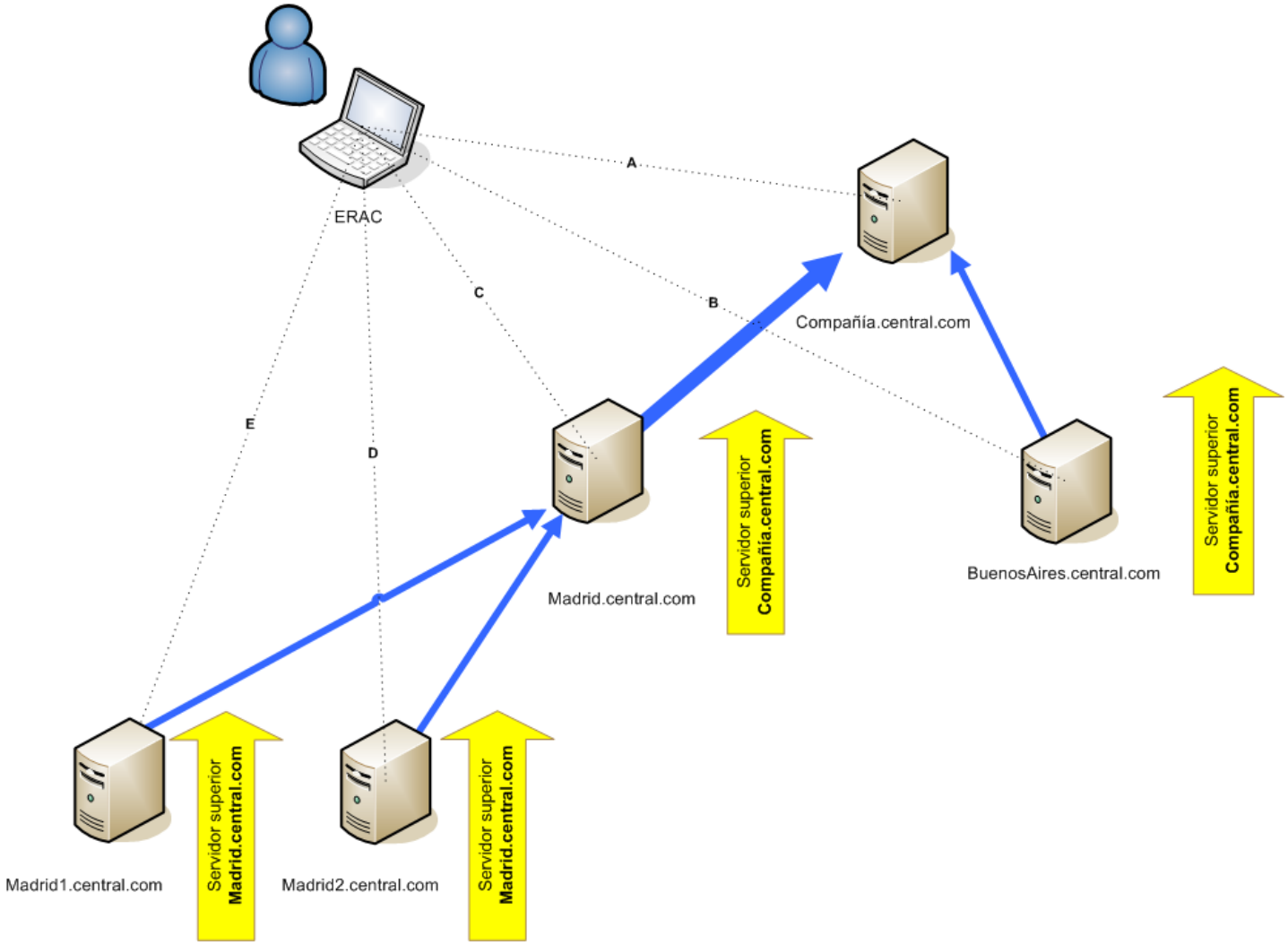
2.3.3 Otros requisitos para los entornos empresariales

En las redes más grandes, se pueden instalar varios ERA Server para realizar instalaciones remotas de ordenadores cliente a partir de servidores más accesibles. Con este fin, ERAS ofrece la *replicación* (consulte los capítulosInstalación en la sede 17 y Sucursal: instalación del ERA Server 17), que permite el reenvío de la información almacenada a un servidor ERAS principal (*servidor superior*). La replicación se puede configurar mediante ERAC.

La característica de replicación es muy útil para empresas que tienen varias sucursales u oficinas remotas. Este sería el escenario de implementación del modelo: Instale ERAS en todas las oficinas y realice la replicación de cada servidor a hacia un ERAS central. La ventaja de esta configuración es especialmente obvia en redes privadas conectadas a través de VPN, que suelen ser más lentas. El administrador sólo tendrá que conectarse a un ERAS central (la comunicación se indica con la letra A en la figura siguiente). No es necesario utilizar la VPN para acceder a departamentos individuales (comunicaciones B, C, D y E). No es necesario utilizar el canal de comunicación más lento gracias a la replicación de ERAS.

La configuración de replicación permite al administrador definir qué información se transferirá automáticamente a los servidores superiores 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 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 a 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.



3. Trabajo con ERAC

3.1 Conexión a ERAS

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

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

Haga clic en el botón **Agregar o Quitar...** para agregar nuevos ERA Server o para modificar los que ya se incluyen en 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 ERAS al iniciarse.
- **Mostrar mensaje cuando se produzca un error de conexión**
  Si se produce un error de comunicación entre ERAC y ERAS, se muestra una alerta.

Son posibles dos tipos de autenticación:

ERA Server

El usuario se autentica con las credenciales de ERAS. No se requiere ninguna contraseña de forma predeterminada para conectarse a un servidor ERAS, pero le recomendamos encarecidamente que se establezca una. Para crear una contraseña para la conexión a ERAS:

Haga clic en **Archivo** > **Cambiar contraseña...** (o en **Herramientas** > **Opciones del servidor** > **Seguridad**) y, a continuación, haga clic en el botón **Cambiar...** situado a la derecha de **Contraseña para la consola**.

Al escribir una contraseña, puede marcar la opción **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...**

Seleccione el tipo de acceso en el menú desplegable **Acceso** (las opciones son **Administrador** o **Sólo lectura**), introduzca la contraseña y haga clic en **Aceptar**.

Dominio de Windows

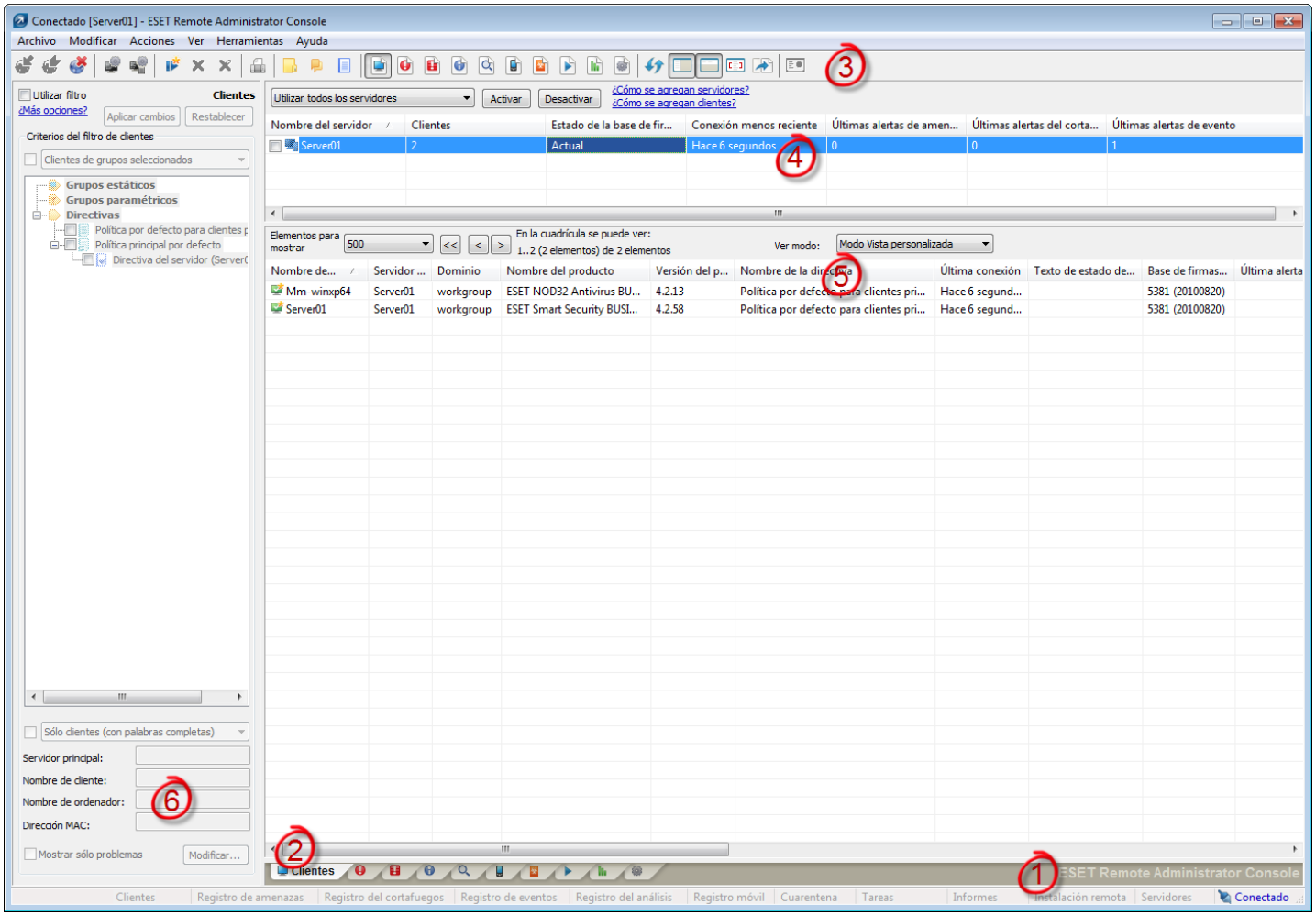
El usuario se autentica con las credenciales del dominio de Windows. Para que la autenticación del dominio de Windows funcione correctamente, es necesario instalar ERAS en la cuenta del dominio de Windows con los derechos adecuados. Active también esta característica en la ficha **Herramientas** > **Opciones del servidor...** > **Avanzadas** > **Modificar configuración avanzada...** > **ESET Remote Administrator** > **ERA Server** > **Configuración** > **Seguridad**:

Permitir autenticación de dominio de Windows: activa o desactiva la autenticación del dominio de Windows.
Grupos de administradores: le permite definir los grupos para los que se activará la autenticación del dominio de Windows.
Grupos de sólo lectura: le permite definir grupos con acceso de sólo lectura.

Cuando se haya establecido la comunicación, el encabezado del programa cambiará a **Conectado [nombre_del_servidor]**.
También puede hacer clic en **Archivo** > **Conectar** para conectarse a ERAS.

NOTA: la comunicación entre ERAC y ERAS está cifrada (AES-256).

3.2 ERAC - Ventana principal



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

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

La información se divide en varias fichas, en orden de importancia (2). En la mayoría de los casos, los datos se pueden ordenar de forma ascendente o descendente, haciendo clic en un atributo (5), y se pueden reorganizar con la operación de arrastrar y soltar. Si se van a procesar varias filas de datos, puede limitarlas con 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 el capítulo Filtrado de la información 21).

La sección Servidor (4) es importante cuando se replican ERA Server. En esta sección se muestra información de resumen sobre la consola a la que está conectado ERAS, así como información sobre ERA Server secundarios o "inferiores". El menú desplegable Servidores de la sección 4 afecta al enfoque de la información mostrada en la sección 5.

- **Usar todos los servidores**
  Muestra información procedente de todos los ERA Server, sección (5).

- **Usar sólo los servidores seleccionados**
  Muestra información procedente de los ERA Server seleccionados, sección (5).

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

Columnas de la sección 4:

- **Nombre de servidor**
  Muestra el nombre del servidor.

- **Clientes**
  Número total de clientes conectados a o presentes en la base de datos del servidor ERAS seleccionado.

- **Rango de bases de firmas de virus**
  Versión de las bases de firmas de virus entre los clientes del servidor ERAS seleccionado.

- **Conexión menos reciente**
  Tiempo que ha transcurrido desde la conexión menos reciente al servidor.

- **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 del cortafuegos.

- **Últimas alertas de suceso**
  Número total de sucesos actuales (consulte el atributo **Último suceso** de la sección 5).

Si actualmente no está conectado, puede hacer clic con el botón derecho del ratón en la sección Servidor (4) y seleccionar **Conectar con este servidor** para conectarse al servidor ERAS seleccionado.

Si la replicación está activada, se mostrará más información en la sección Servidor (4).

Puede acceder a las características más importantes de ERAC desde el menú principal o desde la barra de herramientas de ERAC (3).

La última sección es **Criterios del filtro del ordenador** (6); consulte el capítulo Filtrado de la información 21.

3.3 Filtrado de la información

ERAC proporciona varias herramientas y características que hacen posible que el usuario administre fácilmente los clientes y sucesos. Los sistemas de filtrado avanzado tienen a menudo un valor incalculable, sobre todo en los sistemas que tienen un número elevado de clientes, cuando es necesario agrupar y administrar fácilmente la información mostrada. ERAC incluye varias herramientas que le permiten ordenar y filtrar de forma eficaz la información de los clientes conectados.

3.3.1 Filtro

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

Para activar el filtrado, seleccione la opción **Utilizar filtro**, que se encuentra en la esquina superior izquierda de ERAC. Todas las modificaciones futuras de 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**.

Defina los criterios de filtrado en la sección Criterios del filtro de clientes. Los clientes pueden pertenecer a varios grupos y directivas. La asignación de un cliente a un grupo estático o paramétrico puede resultar muy útil para el filtrado y también para actividades como, por ejemplo, la creación de informes. Para obtener más información sobre la administración de grupos, consulte el capítulo Administrador de grupos 51. El uso de directivas para la segregación de clientes también tiene varias utilidades. Si desea más información sobre la creación y la administración de directivas, consulte el capítulo Directivas 54.

La primera herramienta de filtrado es la selección de grupos y directivas. Hay tres opciones disponibles:

- **Clientes de grupos seleccionados**
  Los clientes de grupos o directivas seleccionados se mostrarán en el panel Clientes.
- **Clientes de grupos no seleccionados**
  Los clientes de grupos o directivas no seleccionados y los clientes que no pertenezcan a ningún grupo se mostrarán

en el panel Clientes.
- **Clientes sin grupos**
  Sólo se mostrarán los clientes que no pertenezcan a ningún grupo o directiva.

NOTA: cuando se selecciona un grupo de la lista, se muestran también todos los subgrupos.

En la parte inferior de la sección Filtro puede especificar otro conjunto de parámetros:
- **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 las tres anteriores.

Los campos Servidor principal, Nombre de cliente, Nombre de ordenador 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.

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 se deben mostrar y haga clic en **Aceptar** para mostrar los clientes que presentan los problemas seleccionados.

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

3.3.2 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 derecho sobre cualquier atributo y seleccionar automáticamente (resaltándolas) todas las demás estaciones de trabajo o servidores que tengan el 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.

- **Mostrar u ocultar columnas**
  Abre la ventana **Opciones de la consola** > **Columnas - Mostrar u ocultar**, donde puede definir las columnas que estarán disponibles en el panel seleccionado.

Las opciones **Ocultar seleccionados/Ocultar no seleccionados** son eficaces si es necesaria una mayor organización después de utilizar los métodos de filtrado anteriores. Para desactivar todos los filtros establecidos por el menú contextual, haga clic en **Ver** > **Vista recortada**, o en el icono de la barra de herramientas de 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, a continuación, haga clic con el botón derecho en cualquier atributo de la columna Nombre de cliente que tiene el valor Joseph. En el menú contextual, haga clic en **Seleccionar por "Joseph"** . A continuación, con la tecla CTRL pulsada, haga clic con el botón derecho y después haga clic en **Seleccionar por "Charles"**. Finalmente, haga clic con el botón derecho 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 diferentes combinaciones.

3.3.3 Modo Vista

En la ficha **Clientes**, se puede ajustar el número de columnas mostradas en el menú desplegable **Modo Vista** situado en la parte derecha de la consola. En el **Modo Vista completa** se muestran todas las columnas y en el **Modo Vista mínima** se muestran únicamente las columnas más importantes. Estos modos están predefinidos y no se pueden modificar. 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 ERAC

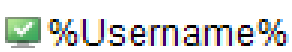
3.4.1 Descripción general de las fichas y los clientes

La mayoría de la información de las fichas está relacionada con los clientes conectados. Los diferentes clientes conectados a ERAS se identifican mediante los atributos siguientes:
Nombre del ordenador (nombre del cliente) + Dirección MAC + Servidor principal

El comportamiento de ERAS en determinadas operaciones de red (como el cambio de nombre de un PC) se puede definir en la configuración avanzada de ERAS. Esto 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 conectan a 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 siguiente). Esta característica permite al administrador detectar fácilmente un ordenador de nueva conexión. Este atributo puede tener significados diferentes en función de los procedimientos operativos del administrador.

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 derecho del ratón en el cliente y seleccionando **Establecer/restablecer indicadores** > **Restablecer el indicador "Nuevo"**. El icono del cliente se cambiará por el mostrado en la figura siguiente y el valor de la columna **Usuario nuevo** cambiará a **No**.



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

Los valores temporales de ERAS se pueden mostrar en modo relativo (*"Hace 2 días"*), en modo absoluto (20.5.2009) o en el modo del sistema (configuración regional).

En la mayoría de los casos, los datos se pueden ordenar de forma ascendente o descendente, haciendo clic en un atributo, y se pueden reorganizar con la operación de arrastrar y soltar.

Al hacer clic en determinados valores, se activan otras fichas para mostrar información más detallada. Por ejemplo, si hace clic en un valor de la columna **Última alerta de amenaza**, el programa abrirá la ficha **Registro de amenazas** para mostrar las entradas del registro de amenazas relacionadas con el cliente en cuestión. Si hace clic en un valor que

contiene demasiada información para mostrar en una vista de ficha, se abrirá una ventana de diálogo con la información detallada del cliente correspondiente.

3.4.2 Replicación e información en fichas individuales

Si ERAC está conectado a un servidor ERAS que actúa como servidor superior, los clientes de los servidores inferiores se mostrarán de forma automática. El tipo de información replicada se puede configurar en el servidor inferior, en **Herramientas** > **Opciones del servidor** > **Replicación** > **Configuración de la replicación "a"**.

En este caso, podrían faltar los datos siguientes:

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

También podría faltar información del programa ESET SysInspector. ESET SysInspector se integra con los productos de generación 4.x y posterior de ESET.

Si no encuentra la información en las ventanas de diálogo del programa, haga clic en el botón **Solicitar** (disponible en **Acciones** > **Propiedades** > **Configuración**). Al hacer clic en este botón, la información que falta se descarga 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.

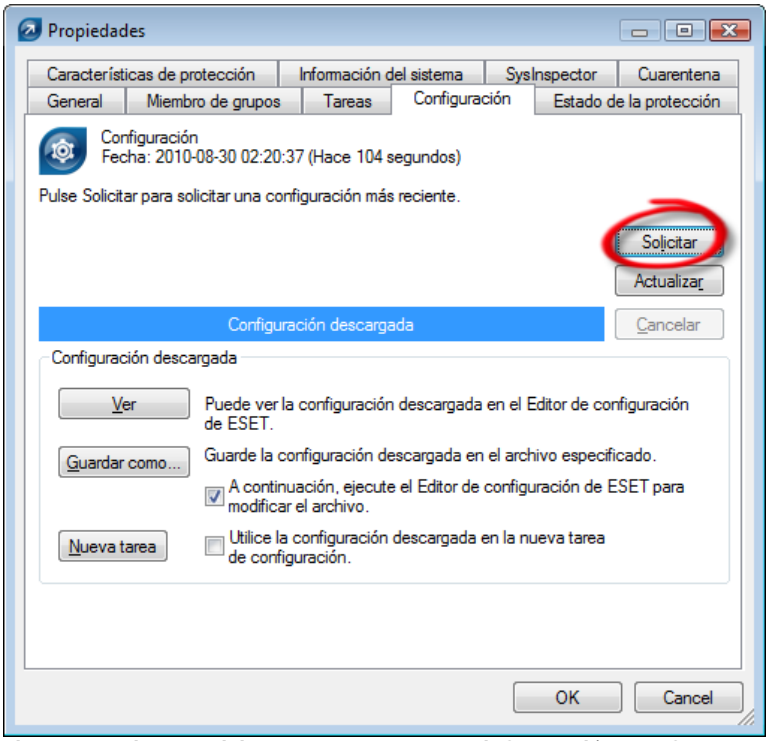


Fig.: haga clic en Solicitar para recuperar la información que falta de ERA Server inferiores.

En el servidor superior, se puede establecer el nivel de los registros que recibirá el servidor (**Herramientas** > **Opciones del servidor** > **Avanzadas** > **Modificar configuración avanzada...** > **ESET Remote Administrator** > **ERA Server** > **Configuración** > **Mantenimiento del servidor** > **Registros de ... que aceptar**).

NOTA: esta opción se aplica a todos los clientes conectados al servidor, y no sólo a los replicados.

3.4.3 Ficha Clientes

En esta ficha se muestra información general acerca de clientes individuales.

Atributo	Descripción
Nombre de cliente	Nombre del cliente (se puede cambiar en la ficha General del cuadro de diálogo de propiedades del cliente)
Nombre de ordenador	Nombre de la estación de trabajo o del servidor (nombre de host)
Dirección MAC	Dirección MAC (adaptador de red)
Servidor principal	Nombre de ERAS con el que un cliente se está comunicando
Dominio	Nombre del dominio o 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 de 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 a 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 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 Alerta y superiores)
Última alerta 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 desinfectados	Número de archivos desinfectados (o eliminados) durante el último análisis a petición
Fecha del último 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 itinerante	Los clientes con este atributo realizarán la tarea "actualizar ahora" cada vez que establezcan una conexión con ERAS (opción recomendada para los portátiles). La actualización sólo se realiza si la base de firmas de virus del cliente no está actualizada.
Nuevo cliente	Ordenador de reciente conexión (consulte el capítulo Descripción general de las fichas y los clientes 23)
Nombre del sistema operativo	Nombre del sistema operativo cliente
Sistema operativo	Plataforma de sistema operativo (Windows, Linux, etc.).
Plataforma de hardware	32 bits o 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 a ERAS (incluida la hora de envío de la información de sistema)
SysInspector	Los clientes con versiones que contengan la herramienta ESET SysInspector pueden enviar

Atributo	Descripción
	registros desde esta aplicación complementaria.
Información personalizada	Información personalizada especificada por el administrador que se mostrará (esta opción se puede configurar en ERAC a través de la ficha **Herramientas > Opciones del servidor... > Avanzadas > Modificar configuración avanzada... > ESET Remote Administrator > ERA Server > Configuración > Otras opciones > Información personalizada del cliente**).
Comentarios	Un comentario corto que describe al 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 **Última alerta de suceso**. Si el administrador procesa esta información y sabe que está obsoleta, se puede borrar haciendo clic con el botón derecho y seleccionando **Borrar información** > **Borrar información de la "Última alerta de amenaza"** o **Borrar información de la "Última alerta de suceso"** . Se eliminará la información relativa al último incidente relacionado con virus o al último suceso del sistema.

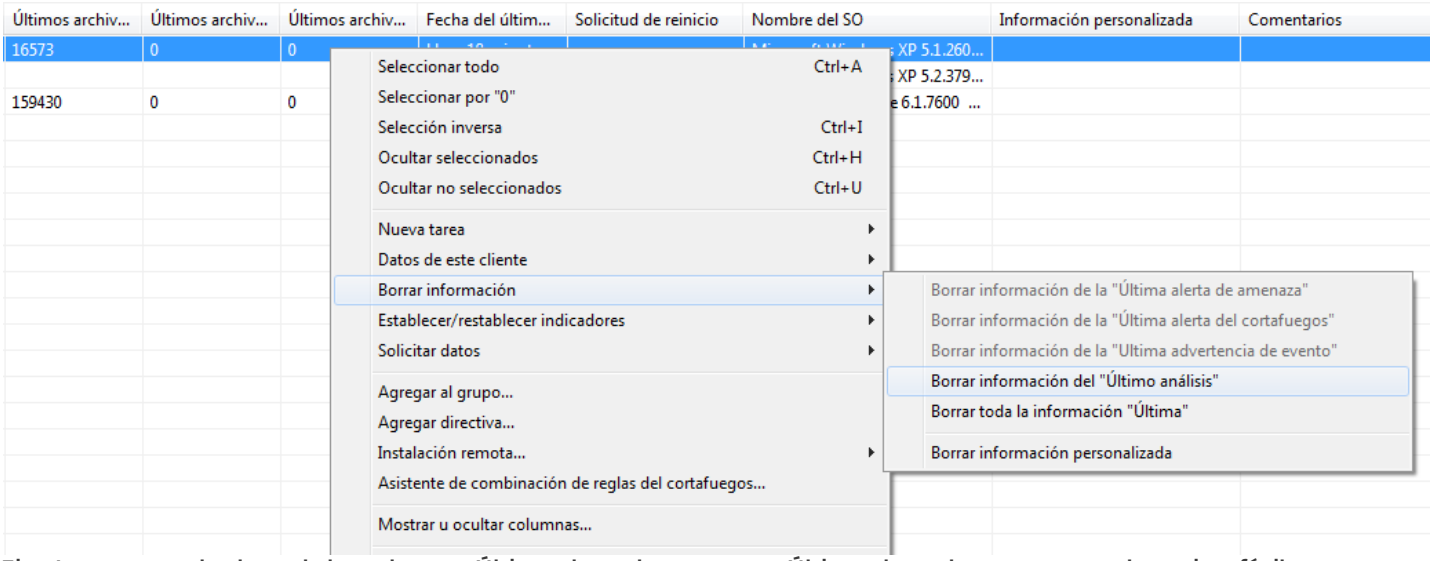


Fig.: Los sucesos obsoletos de las columnas Última alerta de amenaza y Última alerta de suceso se pueden quitar fácilmente.

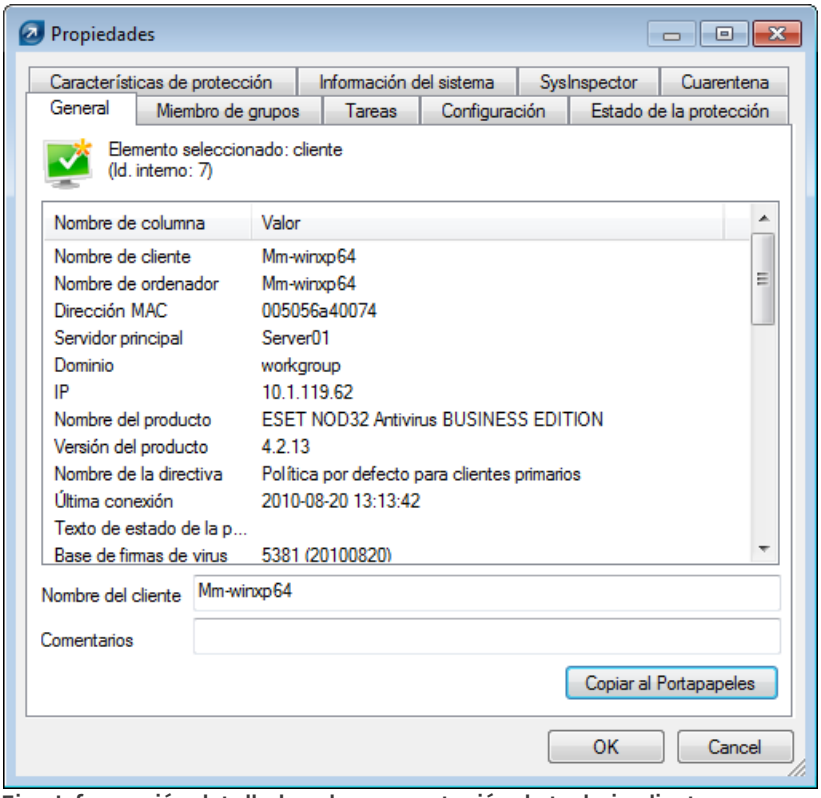


Fig.: Información detallada sobre una estación de trabajo cliente.

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**
En esta ficha se muestra una lista de todos los grupos a los que pertenece el cliente. Para obtener más información, consulte el capítulo Filtrado de la información 21.

- **Tareas**
Tareas relacionadas con el cliente en cuestión. Para obtener más información, consulte el capítulo Tareas 47.

- **Configuración**
Esta ficha le permite ver o exportar a un archivo .xml la configuración actual del cliente. En las secciones posteriores de este manual explicaremos cómo se pueden utilizar los archivos *.xml* para crear una plantilla de configuración para los archivos de configuración *.xml* nuevos o modificados. Para obtener más información, consulte el capítulo Tareas 47.

- **Estado de la protección**
Se trata de una indicación general de estado relativa a todos los programas de ESET. Algunas de estas indicaciones son interactiva y permiten una intervención 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.

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

- **Cuarentena**
Contiene una lista de los archivos en cuarentena. Los archivos en cuarentena se pueden solicitar a un cliente y guardar en un disco local.

3.4.4 Ficha Registro de amenazas

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

Atributo	Descripción
Nombre de cliente	Nombre del cliente que informa de la alerta de amenaza
Nombre de ordenador	Nombre de la estación de trabajo/servidor (nombre de host)
Dirección MAC	Dirección MAC (adaptador de red)
Servidor principal	Nombre de 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
Análisis	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 identificado cuando se produjo 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 de cliente	Nombre del cliente que informa del suceso
Nombre de ordenador	Nombre de la estación de trabajo/servidor (nombre de host)
Dirección MAC	Dirección MAC (adaptador de red)
Servidor principal	Nombre de 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
Objeto	Dirección IP de destino
Protocolo	Protocolo afectado
Regla	Regla del cortafuegos afectado
Aplicación	Aplicación afectada
Usuario	Nombre del usuario identificado cuando se produjo el incidente

3.4.6 Ficha Registro de sucesos

En esta ficha se muestra la lista de todos los sucesos relacionados con el sistema.

Atributo	Descripción
Nombre de cliente	Nombre del cliente que informa del suceso
Nombre de ordenador	Nombre de la estación de trabajo o del servidor (nombre de host)
Dirección MAC	Dirección MAC (adaptador de red)
Servidor principal	Nombre de 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 ordenador a petición que se iniciaron de forma remota, en ordenadores cliente locales, o como tareas programadas.

Atributo	Descripción
Id. de análisis	Id. de la entrada correspondiente en la base de datos (el Id. tiene la forma: *Número de análisis*)
Nombre de cliente	Nombre del cliente en el que se realizó el análisis
Nombre de ordenador	Nombre de la estación de trabajo o del servidor (nombre de host)
Dirección MAC	Dirección MAC (adaptador de red)
Servidor principal	Nombre del ERA Server 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
Objetos analizados	Archivos, carpetas y dispositivos analizados
Analizados	Número de archivos comprobados
Infectados	Número de archivos infectados
Desinfectados	Número de objetos desinfectados (o eliminados)
Estado	Estado del análisis
Usuario	Nombre del usuario identificado cuando se produjo el incidente
Tipo	Tipo de usuario
Análisis	Tipo de análisis
Detalles	Estado del envío del registro de clientes

3.4.8 Ficha Registro móvil

En esta ficha se muestran registros detallados de los teléfonos móviles conectados al ERA Server.

Atributo	Descripción
Id. móvil	Id. de red del dispositivo móvil
Nombre de cliente	Nombre del cliente en el que se realizó la acción
Nombre de ordenador	Nombre de la estación de trabajo o del servidor (nombre de host)
Dirección MAC	Dirección MAC (adaptador de red)
Servidor principal	Nombre del ERA Server 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 en que se produjo el suceso en un cliente
Nivel	Nivel de alerta
Tipo de registro	Tipo de un registro (p. ej. Registro de auditoría de seguridad, Registro de antispam para SMS)
Suceso	Descripción del suceso
Tipo de objeto	Objeto con el que se relaciona el suceso (p. ej. SMS, archivo, etc.)
Nombre del objeto	Objeto determinado con el que se relaciona el suceso (p. ej. número de teléfono del remitente del SMS, ruta al archivo, etc.)
Acción	Acción realizada (o error detectado) durante el suceso

3.4.9 Ficha Cuarentena

En esta ficha de recopilan todas las entradas de cuarentena de la red.

Atributo	Descripción
Id. de cuarentena	Número de Id. del objeto en cuarentena asignado en orden de ocurrencia
Hash	Código hash del archivo
Fecha de recepción	Fecha y hora a la que ERAS registra el suceso de análisis
Primera ocurrencia	Tiempo transcurrido desde la primera ocurrencia del elemento en cuarentena
Última ocurrencia	Tiempo transcurrido desde la última ocurrencia del elemento en cuarentena
Nombre del objeto	Generalmente, una carpeta en la que se ubica la infección
Nombre de archivo	Nombre del archivo en cuarentena
Extensión	Tipo de extensión del archivo en cuarentena
Tamaño	Tamaño del archivo en cuarentena
Detalle	Motivo de la cuarentena; normalmente es una descripción del tipo de amenaza
Recuento de clientes	Número de clientes que tienen el objeto en cuarentena
Coincidencias	Número de veces que se puso el objeto en cuarentena
Archivo	Indica si se solicitó la descarga del objeto al servidor

3.4.10 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 al cliente (escrito por el administrador)

3.4.11 Ficha Informes

Esta ficha contiene características que se pueden usar para archivar la actividad en la red durante ciertos períodos de tiempo. La ficha **Informes** se utiliza para organizar la información estadística en forma de gráfico o tabla. Para obtener más información, consulte el capítulo Informes 74.

3.4.12 Ficha Instalación remota

En esta ficha se proporcionan opciones para varios métodos de instalación remota de ESET Smart Security o ESET NOD32 Antivirus en clientes. Para obtener más información, consulte el capítulo Instalación remota 35.

3.5 Configuración de la ERA Console

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 ERAC a ERAS. Para obtener más detalles, consulte el capítulo Conexión a ERAS 19.

3.5.2 Columnas - Ficha Mostrar u ocultar

Esta ficha permite especificar los atributos (columnas) que se muestran en las fichas individuales. Los cambios se reflejarán en el modo de vista personalizada (ficha **Clientes**). Los demás modos no se pueden 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 le permite especificar el directorio en el que ERAC guardará los informes descargados de 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 tras 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 búsqueda de versiones nuevas de ESET Remote Administrator. Recomendamos utilizar el valor predeterminado, **Mensualmente**. Si hay una versión nueva disponible, 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** > **Mostrar líneas de la cuadrícula**
  Seleccione esta opción para separar las celdas individuales de todas las fichas por cuadrícula.

- **Otras opciones** > **Mostrar preferentemente el cliente como "Servidor/Nombre" que como "Servidor/Ordenador/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 ERA Console 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 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 y el botón Modificar para definir los sucesos que desencadenarán un cambio en el color del icono de ERAC en el área de notificación.

Si la consola ERAC del PC del administrador va estar conectada de forma permanente a ERAS, se recomienda desactivar la opción **Mostrar en la barra de tareas al estar minimizado** y dejar la consola minimizada cuando esté inactiva. Si se produce algún problema, el icono del área de notificación se volverá rojo para indicar que el administrador debe intervenir. También se recomienda ajustar la opción **Utilizar icono de Systray resaltado al encontrar clientes problemáticos** para especificar los sucesos que desencadenarán un cambio de color en el icono de ERAC. Sin embargo, ERAC se desconectará si se activa la compresión de la base de datos en el servidor.

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

3.6 Modos de visualización

ERAC ofrece a los usuarios dos modos de visualización:

- Modo administrativo
- Modo de sólo lectura

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

El modo de sólo lectura resulta adecuado para ver el estado de las soluciones cliente de ESET que se conectan a ERAS; no permite la creación de tareas para estaciones de trabajo cliente, 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 modificar la configuración de ERAC y generar 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 a 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 a ERAS y 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 ESET Configuration Editor

ESET Configuration Editor es un componente importante de ERAC y se usa para distintos fines. Entre los más importantes, se encuentra la creación de los siguientes elementos:

- Configuraciones predefinidas para los paquetes de instalación
- Configuraciones enviadas como tareas o directivas a los clientes
- Archivo de configuración (.xml) general

Configuration Editor forma parte de ERAC y consta principalmente de archivos *cfgedit.**.

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

La estructura que utiliza Configuration Editor es 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 ERAS y ERAC de forma periódica.

Alerta: Configuration Editor le permite modificar cualquier archivo *.xml*. No modifique ni sobrescriba el archivo *cfgedit.xml* original.

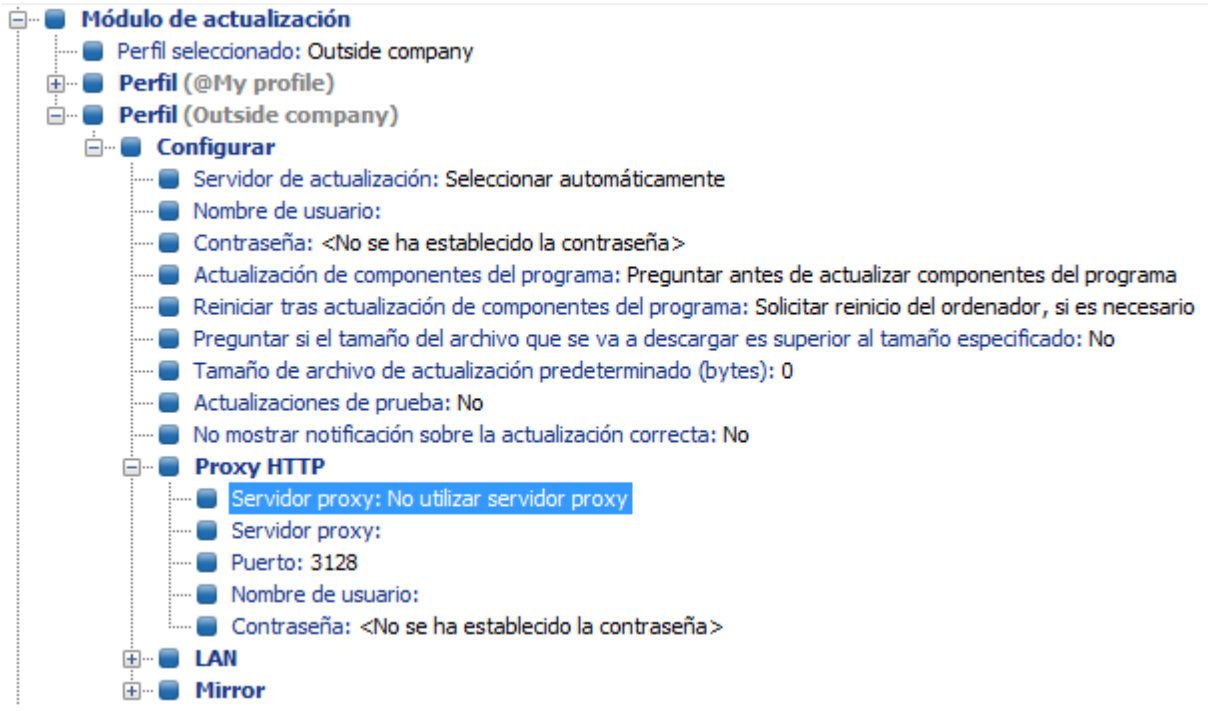
Para que Configuration Editor funcione, deben estar disponibles los archivos siguientes: *eguiEpfw.dll*, *cfgeditLang.dll*, *eguiEpfwLang.dll* y *eset.chm*.

3.7.1 Capa de configuración

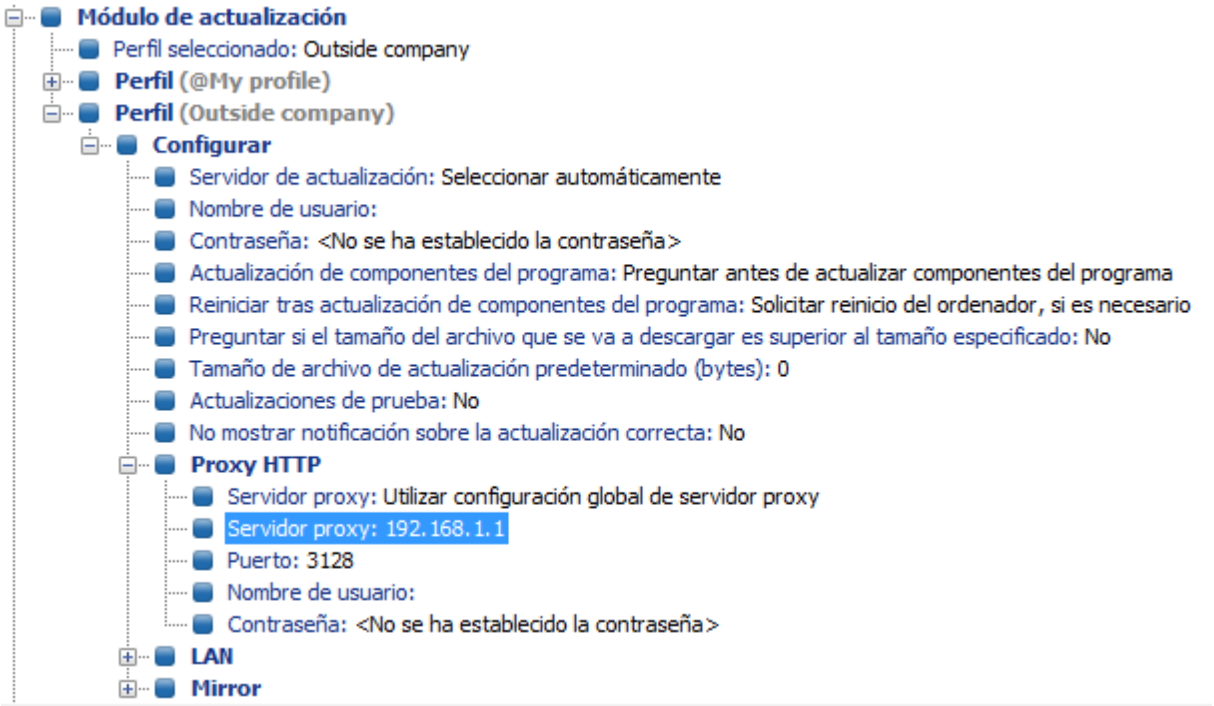
Si se cambia un valor en Configuration Editor, el cambio se muestra con un símbolo azul. Las entradas con icono gris no se han modificado y no se escribirán en la nueva configuración de salida *.xml*.

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

En la figura siguiente se muestra un ejemplo. En esta configuración, el nombre de usuario *EAV-12345678* y la contraseña se insertan y se prohibe el uso de un servidor proxy.



La segunda configuración (mostrada en la figura siguiente) enviada a los clientes garantiza la conservación de las modificaciones anteriores, incluidos el nombre de usuario *EAV-12345678* y la contraseña. Esta configuración también permite utilizar un servidor proxy, para el que define una dirección y un puerto.



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 de ESET Configuration Editor:

- **ESET Smart Security**, **ESET NOD32 Antivirus** > **Kernel de ESET** > **Configuración** > **Administración remota**
  Desde aquí puede activar la comunicación entre ordenadores cliente y ERAS (**Conectar con servidor de administración remota**). Especifique el nombre o dirección IP de 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 especificada en ERAS. Para obtener más información, consulte la opción **Contraseña para clientes** en el capítulo Ficha Seguridad 77. También encontrará información adicional sobre la configuración de contraseñas en esta sección.

- **Kernel de ESET** > **Configuración** > **Claves de licencia**
  Los ordenadores cliente 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**
  En esta sección se 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 implementan 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 se desactiva por completo. 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 a ERAS, que a su vez los remite a los servidores de ESET. Por ello es necesario configurar correctamente el servidor proxy en ERAS (**Herramientas > Opciones del servidor > Avanzadas > Modificar configuración avanzada > ERA Server > Configuración > Servidor proxy**).

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

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

NOTA: de forma predeterminada, todas las soluciones de seguridad de ESET contienen distintas tareas predefinidas (como 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 tareas nuevas.

- **Kernel de ESET** > **Configuración** > **Valores predeterminados de la interfaz de usuario**
  Los ajustes de Valores predeterminados de la interfaz de usuario (es decir, **Mostrar pantalla de inicio**/**No mostrar pantalla de inicio**) sólo modifican la configuración predeterminada del cliente. Después, la configuración del cliente se puede administrar de forma individual para cada usuario y no se puede modificar remotamente. Para cambiar la configuración de forma remita, establezca la opción **Suprimir configuración de usuario** en **Sí**. La opción **Suprimir configuración de usuario** sólo está disponible para los clientes que ejecutan la versión 4.0 o una versión posterior de los productos de seguridad de ESET.

- **Actualizar**
  Esta sección de Configuration Editor le permite definir el modo de aplicación de los perfiles de actualización. Normalmente, basta con modificar el predefinido **Mi perfil** y cambiar los ajustes **Servidor de actualización**, **Nombre de usuario** y **Contraseña**. Si el servidor de actualización se establece en **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 (Mirror), consulte el capítulo Servidor Mirror 78. Para obtener más información acerca del programador de tareas, consulte el capítulo Programador de Tareas 92.

NOTA: en los dispositivos portátiles (como los ordenadores portátiles), se pueden configurar dos perfiles. Uno para ofrecer actualizaciones desde el servidor Mirror y otro para descargar las actualizaciones directamente desde los servidores de ESET. Para obtener más información, consulte el apartado Actualización combinada para portátiles 95 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 las estaciones de trabajo o de forma remota, desde ERAS. En este capítulo también se ponen de relieve métodos alternativos para la instalación remota.

NOTA: aunque es factible desde un punto de vista técnico, no recomendamos el uso de la característica de 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 ordenador en el que se instalará el producto de seguridad de ESET. Este método no requiere mayor preparación y es adecuado para redes de ordenadores pequeñas o para casos en los que no se utilice 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 Mirror, etc.), modo silencioso, análisis programado, etc., durante la instalación o después.

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 4.x: Descargue el archivo instalación (p. ej., *ess_nt32_enu.msi*) de *eset.com* y cree su propio paquete de instalación en el **Editor de paquetes de instalación**. Edite o seleccione la configuración que desee asociar a este paquete, pulse el botón **Copiar...** situado junto al campo **Paquete para sistemas Windows NT de xx bits** y guarde el paquete como **Archivo MSI de instalación de ESET con configuración (*.msi)**.

  NOTA: si se agrega una configuración al archivo de instalación *.msi*, la firma digital de este archivo dejará de ser válida.

  Además, los pasos de la versión 3.x son aplicables también a la versión 4.x.

- Versión 3.x: Descargue el archivo de instalación (p. ej., *ess_nt32_enu.msi*) de *eset.com*. Copie el archivo de configuración (*cfg.xml*) en el directorio donde se encuentra 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 (p. ej., *ndntenst.exe*) de *eset.com*. Extraiga el archivo descargado en una carpeta mediante un programa de extracción de archivos, como WinRAR. La carpeta contendrá los archivos de instalación, incluido el archivo *setup.exe*. Copie el archivo de configuración *nod32.xml* en la carpeta. Ejecute el archivo *setup.exe*. Se aplicará automáticamente la configuración de *nod32.xml*. Si el archivo de configuración *.xml* tiene un nombre diferente o se encuentra en 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 scripts de inicio de sesión
- Instalación remota por correo electrónico
- Actualizar

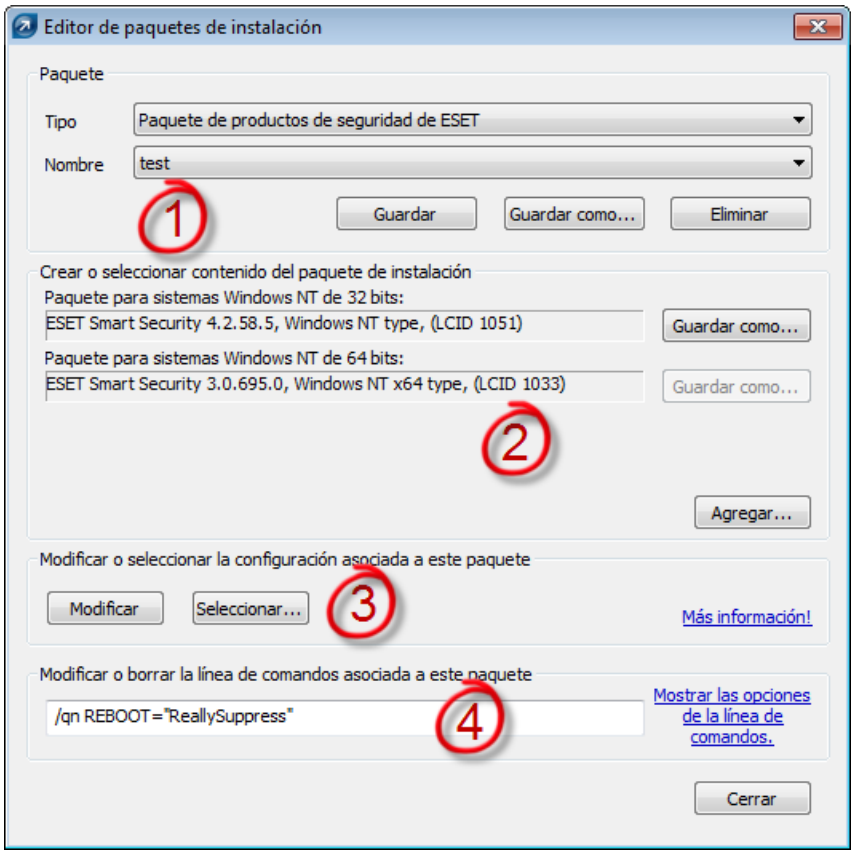
La instalación remota mediante ERA consta de los pasos siguientes:

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

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

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

Para iniciar paquetes de instalación desde ERAC, haga clic en la ficha **Instalación remota**, seleccione la ficha **Ordenadores** y haga clic con el botón derecha en cualquier punto del contenido. Seleccione **Administrar paquetes** en el menú contextual.



Cada paquete de instalación se define mediante un nombre. Vea (1) en la figura anterior. Las secciones restantes de la ventana de diálogo hacen referencia al contenido del paquete, que se aplica tras su correcta entrega a una estación de trabajo de 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 características adicionales de ERA. Además de la instalación remota, los productos de seguridad de ESET permiten también la desinstalación de forma remota con la opción **Desinstalar productos de seguridad de ESET y NOD32 versión 2**. Asimismo, se puede realizar la instalación remota de una aplicación externa con la opción **Paquete personalizado**. Esto es muy útil cuando se quieren ejecutar varios scripts y archivos ejecutables en la máquina remota, como herramientas de desinstalación de productos de seguridad de terceros o herramientas de desinfección independientes. Puede especificar parámetros personalizados de la línea de comandos para su uso con el **Archivo de entrada del paquete**. Consulte el capítulo Instalación de productos de terceros con ERA 97 para obtener más detalles.

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 de destino y ERAS. El agente de instalador remoto de ESET se denomina *einstaller.exe* y contiene el nombre de ERAS, además del nombre y el tipo del paquete al que pertenece. En los capítulos siguientes se ofrece 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 un porcentaje en una barra de progreso.
- **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="password"**
  Debe agregar 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 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, que son necesarias para el correcto funcionamiento de ERA. Este parámetro se puede utilizar siempre, aunque 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 a partir de un paquete de instalación existente y guardado (botón **Guardar como...**). Estos paquetes de instalación se pueden ejecutar en estaciones de trabajo cliente donde se vaya a instalar el programa. El usuario sólo tendrá que ejecutar el paquete para que el producto se instale sin volver a conectarse a ERAS durante la instalación.

NOTA: si se agrega una configuración al archivo de instalación *.msi*, la firma digital de este archivo dejará de ser válida.

Importante: en Microsoft Windows Vista y versiones posteriores, recomendamos encarecidamente la instalación remota silenciosa (parámetro */qn*, */qb*). De lo contrario, la interacción con un usuario podría provocar un fallo en la instalación remota por tiempo de espera excedido.

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, la estación de trabajo cliente está sujeta a condiciones más estrictas que las exigidas en una instalación directa. La instalación remota requiere el cumplimiento de las condiciones siguientes:

- 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 de ERAS y 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 se puede dejar en blanco)
- Utilizar uso compartido simple de archivos desactivado
- Servicio del servidor activado
- Servicio Registro remoto activado

NOTA: las versiones recientes de Microsoft Windows (Windows Vista, Windows Server 2008 y Windows 7) aplican directivas de seguridad que limitan los permisos de las cuentas de usuario local, por lo que es posible que el usuario no pueda ejecutar operaciones de red específicas. Si el servicio de ERA se ejecuta en una cuenta de usuario local, es posible que se produzcan problemas de instalación impulsada en determinadas configuraciones de red (p. ej., durante la instalación remota desde un dominio en un grupo de trabajo). Si se utiliza Windows Vista, Windows Server 2008 o Windows 7, es recomendable ejecutar el servicio de ERA en cuentas con suficientes derechos de red. Para especificar la cuenta de usuario donde desea que se ejecute ERA, vaya a **Inicio** ' **Panel de control** ' **Herramientas administrativas** ' **Servicios**. Seleccione el servicio de ESET Remote Administrator Server en la lista y haga clic en la ficha **Inicio de sesión** . ESET Remote Administrator 4 incorpora esta configuración en la situación de instalación avanzada, de modo que debe seleccionar **Avanzadas** ' **Instalación completa personalizada** durante la instalación. Si está utilizando la instalación impulsada en Windows Vista, Windows Server 2008 o en las estaciones de trabajo de destino de Windows 7, asegúrese de que su ERA Server así como las estaciones de trabajo de destino están en un dominio.

Le recomendamos encarecidamente que compruebe todos los requisitos antes de la instalación, especialmente si hay varias estaciones de trabajo en la red (en la ficha **Instalación remota**, seleccione la ficha **Ordenadores**, haga clic con el botón derecho en los clientes pertinentes y seleccione **Diagnósticos de la instalación impulsada** en el menú contextual).

4.2.2 Configuración del entorno para la instalación remota

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

En la sección **Vista de red** de la ficha **Instalación remota** se proporciona una vista personalizable de la red. La red se puede explorar de dos maneras.

Consola

En la vista **Consola** se proporciona una búsqueda de NetBios estándar desde el ordenador donde está instalada ERAC. Muestra todos los dominios y grupos de trabajo disponibles que se pueden (des)marcar para filtrar la vista.

Servidor

En la vista **Servidor** se proporcionan más opciones de filtrado. Además de la búsqueda de NetBios, se pueden visualizar ordenadores con filtros de Active Directory, clientes de ERA existentes o personalizados.

Los filtros personalizados constan de dos elementos: la **Lista personalizada** y la **Búsqueda de IP**. Ambos elementos le permiten crear sus propios grupos de forma manual.
En la **Lista personalizada** se pueden agregar ordenadores a un grupo manualmente, escribiendo sus nombres en la sección **Ordenadores del grupo** o importándolos desde un archivo *.txt*. En ambos casos, los nombres de ordenador deben escribirse de uno o en uno, con formato de lista.
En la sección **Búsqueda de IP** se pueden crear rangos de IP y grupos de rangos de IP, donde el rango de IP actúa como criterio de filtrado.

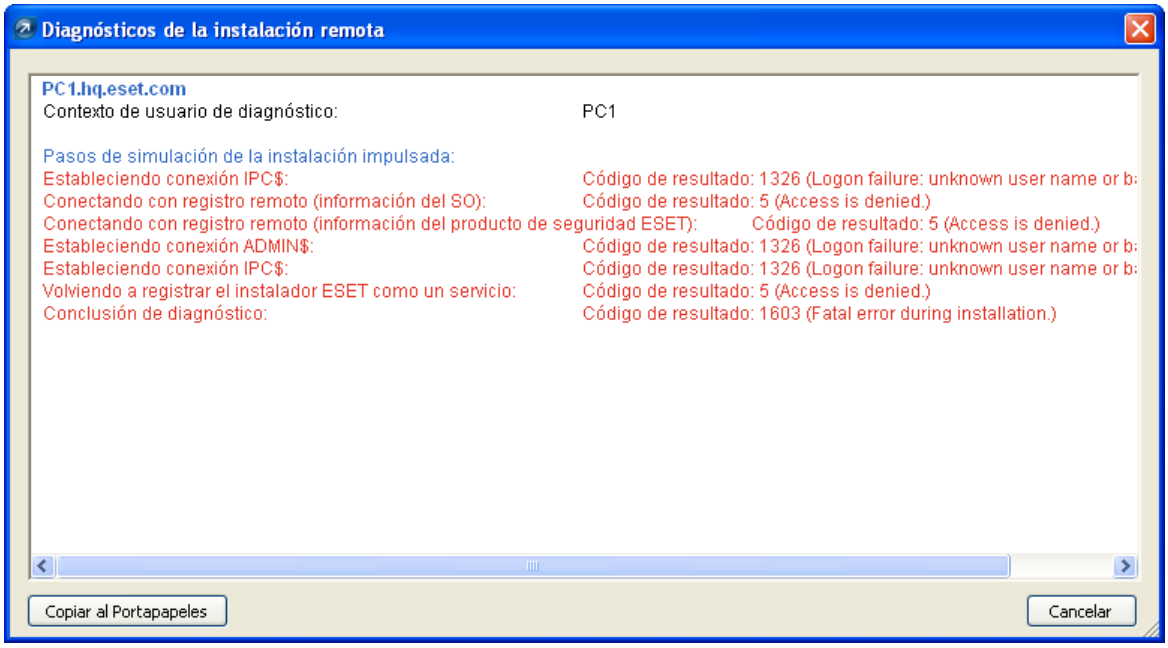
NOTA: en las secciones Consola y Servidor se especifica si la búsqueda en los ordenadores se realiza desde ERAS o desde ERAC. Es recomendable tener en cuenta este aspecto cuando se realiza la conexión a ERAS desde una red diferente.

En la sección **Opciones de filtro** se proporcionan dos opciones de filtrado adicionales:

Ordenadores no registrados: muestra los ordenadores que no se encuentran en la base de datos del servidor actual.

Clientes con alerta de última conexión: muestra los ordenadores que se enumeran en la base de datos del servidor actual y presentan la alerta de última conexión.

Una vez que haya configurado todas las condiciones necesarias en la secciones **Vista de red** y **Opciones de filtro**, verá una lista de las estaciones de trabajo adecuadas para la instalación de una solución cliente en el lado derecho de la ficha **Ordenadores**. Los diagnósticos de la instalación impulsada se pueden ejecutar en los ordenadores de la lista, haciendo clic con el botón derecho del ratón en los ordenadores seleccionados para seleccionar **Diagnósticos de la instalación impulsada** en el menú contextual. Los diagnósticos le ayudan a comprobar los requisitos de la instalación e identificar los problemas potenciales.



4.2.3 Instalación impulsada remota

Este método de instalación remota impulsa las soluciones cliente de ESET a ordenadores de destino remotos. Los ordenadores de destino deben estar en línea. En el supuesto de que todas las estaciones de trabajo estén activadas, el método de instalación impulsada resulta el más efectivo. Antes de iniciar una instalación impulsada, descargue 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. Antes de iniciar la instalación, consulte el capítulo Requisitos 38.

Para iniciar una instalación impulsada, siga estos pasos:

1) Cuando se especifiquen los ordenadores adecuados para la instalación remota en la ficha **Ordenadores**, puede seleccionar los ordenadores que desee y ejecutar una tarea de instalación impulsada haciendo clic con el botón derecho del ratón en la ventana y seleccionando **Instalación remota** en el menú contextual.

2) Establezca la información de inicio de sesión de los ordenadores en la lista (**Establecer**, **Establecer todas**). Para realizar esta operación, utilice una cuenta que disponga de derecho de administrador. En este paso puede seguir agregando clientes a la lista, con la característica especial **Agregar clientes**.

3) Seleccione el paquete de instalación que desee para entregar a la estaciones de trabajo cliente de destino.

4) Establezca la hora a la que se debe ejecutar la tarea y pulse **Finalizar**.

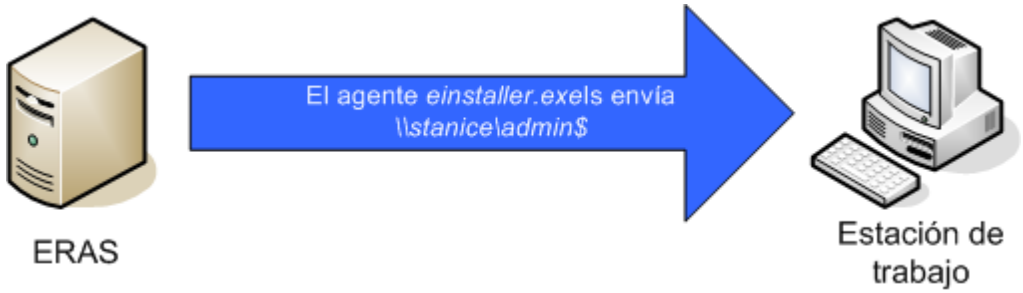
El estado de la tarea de instalación impulsada se puede ver en la ficha **Tareas de instalación**. Para obtener detalles de los resultados de diagnóstico, consulte la tarea que desee y pulse F4. La ventana **Propiedades** se muestra en la ficha

Detalles, donde se pueden ver los resultados del diagnóstico de instalación remota con la opción **Ver todos los registros/Ver registros seleccionados**.

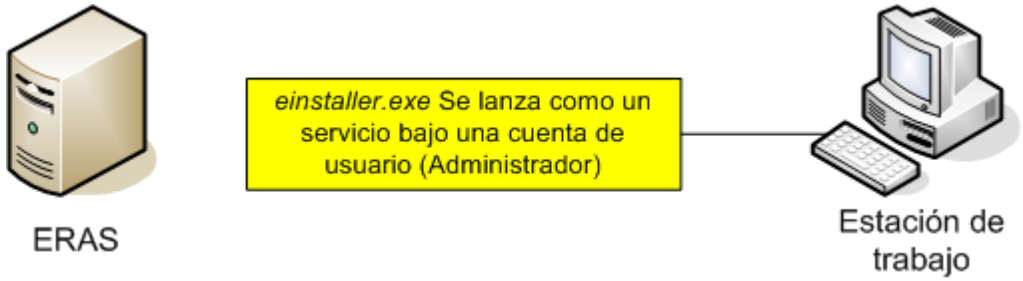
NOTA: el número máximo de subprocesos simultáneos de instalación impulsada está establecido, de forma predeterminada, en 20. Si envía una tarea de instalación impulsada a un número mayor de ordenadores, los ordenadores que sobrepasen este límite se pondrán en cola hasta que los subprocesos estén libres. Por motivos de rendimiento, no es recomendable aumentar este valor. No obstante, si lo cree necesario, puede cambiar el límite en el editor de configuración (**ESET Remote Administrator** > **ERA Server** > **Configuración** > **Instalación remota**).

A continuación se describen los detalles del proceso de instalación remota:

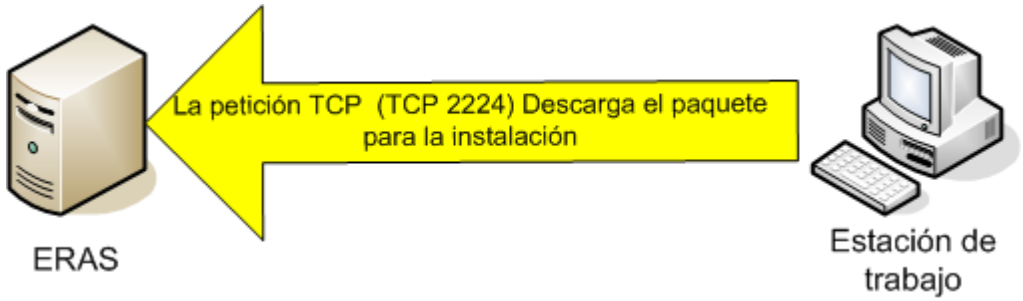
5) ERAS envía el agente *einstaller.exe* a la estación de trabajo con la ayuda del recurso compartido administrativo admin$.



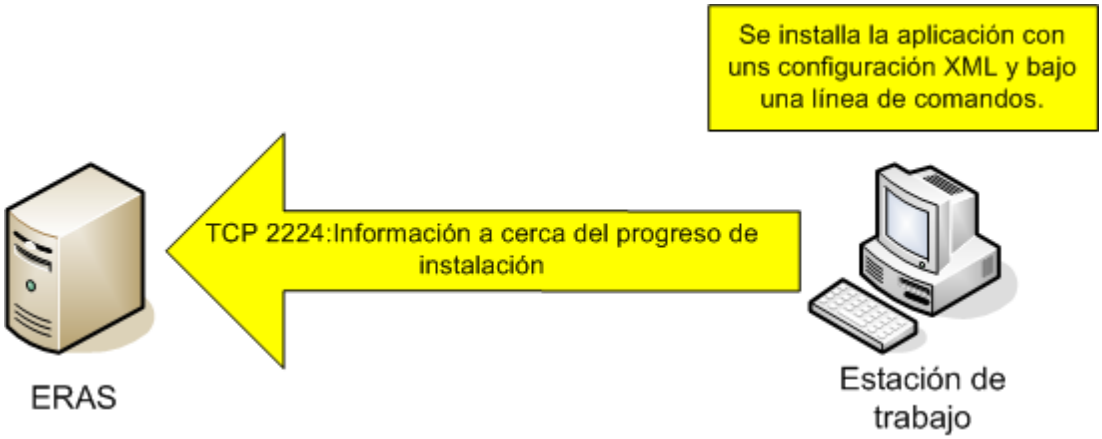
6) El agente inicia un servicio en la cuenta del sistema.



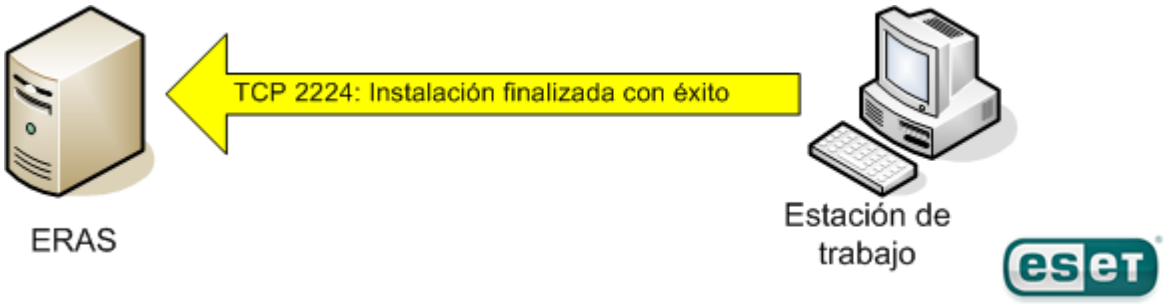
7) El agente establece la comunicación con su ERAS principal y descarga el paquete de instalación correspondiente en el puerto TCP 2224.



8) El agente instala el paquete en la cuenta de administrador definida en el paso 2. También se aplican la configuración .*xml* correspondiente y los parámetros de la línea de comandos.



9) Inmediatamente después de la finalización de la instalación, el agente envía un mensaje a ERAS. Algunos productos de seguridad de ESET requerirán el reinicio; el ordenador lo solicitará en caso necesario.



El menú contextual (clic con el botón derecho) de la ventana **Ordenadores** ofrece las opciones siguientes:

- **Administrar paquetes**
  Ejecuta el **Editor de paquetes de instalación**. Consulte el capítulo Instalación remota 35 para obtener más detalles.

- **Actualizar cliente**
  Ejecuta la tarea de actualización. Utilice esta opción si desea instalar una versión más reciente de ESS/EAV encima de la anterior.

- **Diagnósticos de la instalación impulsada**
  Comprueba la disponibilidad de los clientes y servicios que se utilizarán durante la instalación remota. Para obtener más información, consulte el capítulo Configuración del entorno para la instalación remota 38.

- **Instalación impulsada**
  Ejecuta la tarea de instalación remota.

- **Exportar a carpeta o script de inicio de sesión**
  Consulte el capítulo Instalación remota por correo electrónico/inicio de sesión 42 para obtener más detalles.

- **Enviar por correo electrónico**
  Consulte el capítulo Instalación remota por correo electrónico/inicio de sesión 42 para obtener más detalles.

- **Establecer inicio de sesión predeterminado para instalaciones por medio de correo electrónico o scripts de inicio de sesión**
  Abre la ventana **Inicio de sesión predeterminado**, donde se puede especificar el nombre de usuario y la contraseña de una cuenta de administrador de los ordenadores de destino.

- **Propiedades**
  Abre la ventana **Propiedades del cliente**, donde se encuentra toda la información importante del cliente.

Para obtener más información sobre las demás opciones del menú contextual, consulte el capítulo Menú contextual 22.

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 divergen 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 del script de inicio de sesión o por correo electrónico. El agente *einstaller.exe* también se puede utilizar de forma individual y ejecutar a través de otros métodos (para obtener más información, consulte el capítulo Instalación remota personalizada 44).
El método de inicio de sesión es el ideal para portátiles que se utilizan a menudo fuera de la red local. La instalación se realiza tras el inicio de sesión en el dominio. Para estos dispositivos, se sugiere el método de script de inicio de sesión.

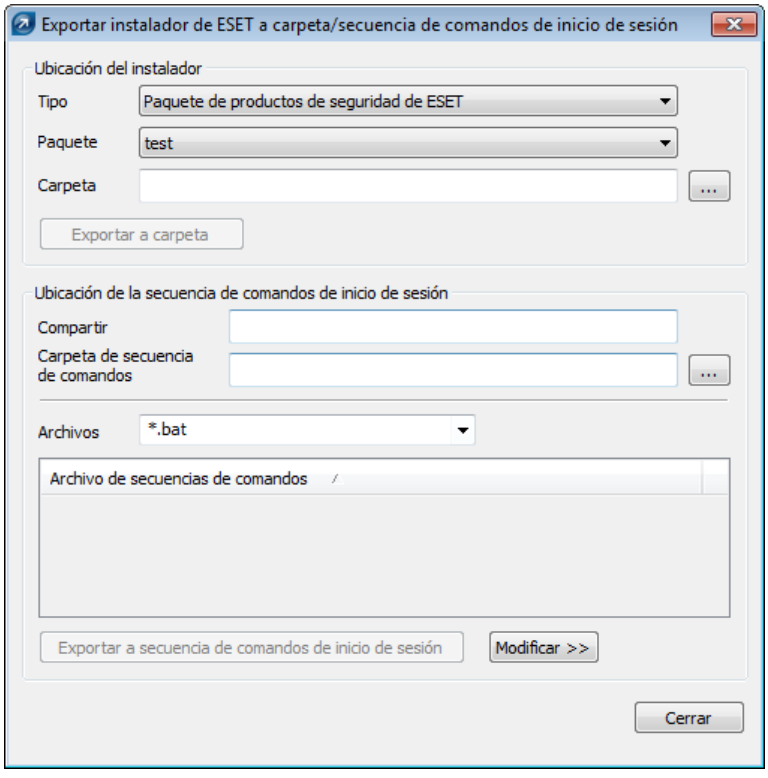
El script de inicio de sesión se ejecuta automáticamente cuando el usuario inicia sesión, mientras que el método de correo electrónico requiere la intervención del usuario, que deberá iniciar el agente einstaller.exe incluido como archivo adjunto en el correo electrónico. Si se inicia de forma repetida, einstaller.exe no desencadena otra instalación de soluciones cliente de ESET. Para obtener más información, consulte el capítulo Cómo evitar instalaciones repetidas 45.

La línea de llamada del agente *einstaller.exe* del script 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 medio de cualquier cliente de correo electrónico. Independientemente del método utilizado, asegúrese de utilizar el archivo *einstaller.exe* correcto.

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

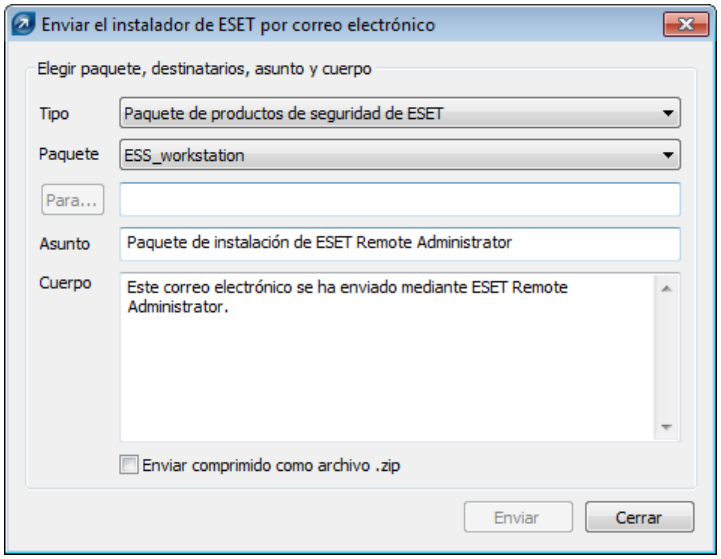
Introduzca la ruta de acceso a *einstaller.exe* en el script de inicio de sesión:

1) Haga clic con el botón derecho del ratón sobre una entrada de la ficha **Instalación remota**, haga clic en **Exportar a carpeta o script de inicio de sesión** y seleccione el **Tipo** y el nombre del **Paquete** que se instalará.
2) Haga clic en el botón ..., situado junto a **Carpeta**, y seleccione el directorio de la red donde el archivo *einstaller.exe* se ubicará y estará disponible; a continuación, haga clic en **Aceptar**.
3) En el campo **Compartir**, asegúrese de que la ruta sea correcta y, si es necesario, modifíquela.
4) Haga clic en el botón **...**, situado junto a **Carpeta de scripts**, para seleccionar la carpeta donde se encuentra el script y, si es necesario, modifique la máscara (**Archivos**).
5) En la sección **Archivos**, seleccione el archivo en que se insertará la línea (invocando a *einstaller.exe*).
6) Haga clic en **Exportar a script de inicio de sesión** para insertar la línea.
7) Puede modificar la ubicación de la línea haciendo clic en **Modificar >>** y guardarla con el botón **Guardar**.

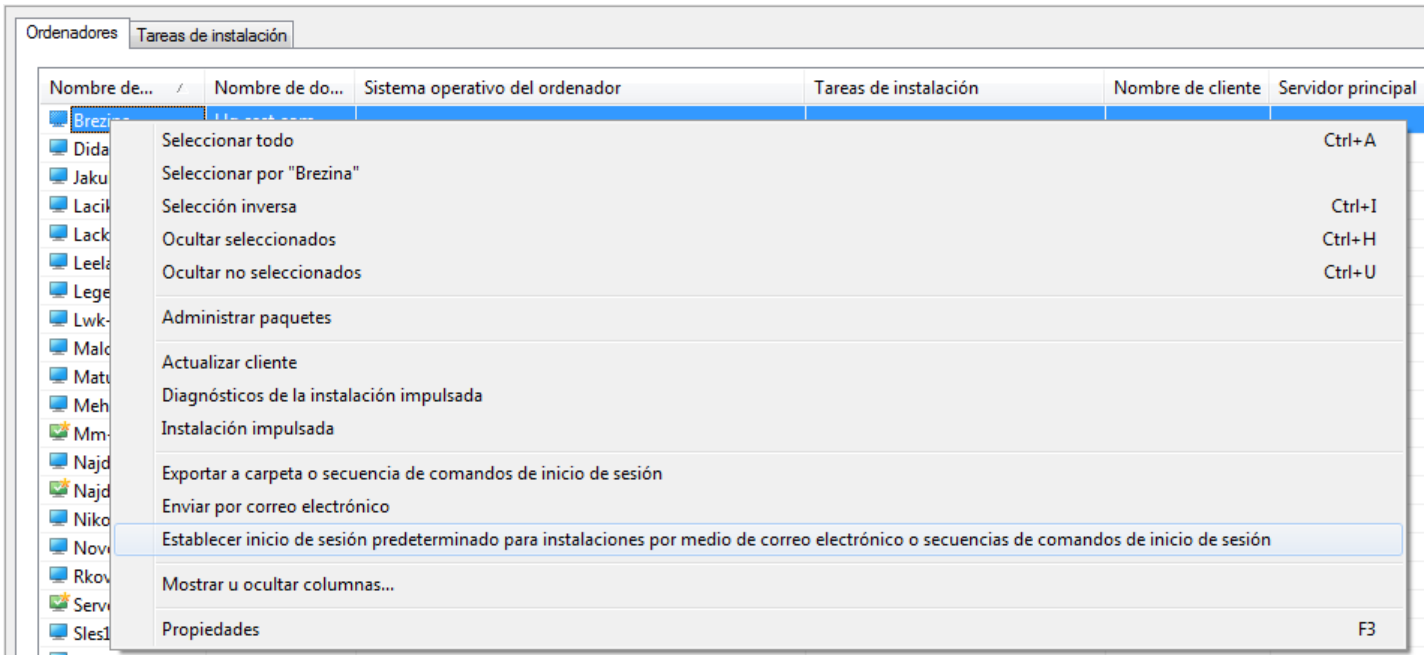


Para adjuntar el agente (*einstaller.exe*) al correo electrónico:

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



Durante el proceso de instalación remota, se vuelve a establecer la conexión con ERAS y el agente (*einstaller.exe*) adopta los parámetros de configuración de **Establecer inicio de sesión predeterminado para instalaciones por medio de correo electrónico o scripts de inicio de sesión** en el menú contextual.



El nombre de usuario y la contraseña de la cuenta con la que se va a ejecutar la instalación del paquete deben pertenecer a una cuenta con derechos de administrador o, preferiblemente, una cuenta de administrador de dominio. Los valores insertados en la ventana de diálogo **Inicio de sesión predeterminado...** se olvidan tras cada reinicio del servicio (ERAS).

4.2.5 Instalación remota personalizada

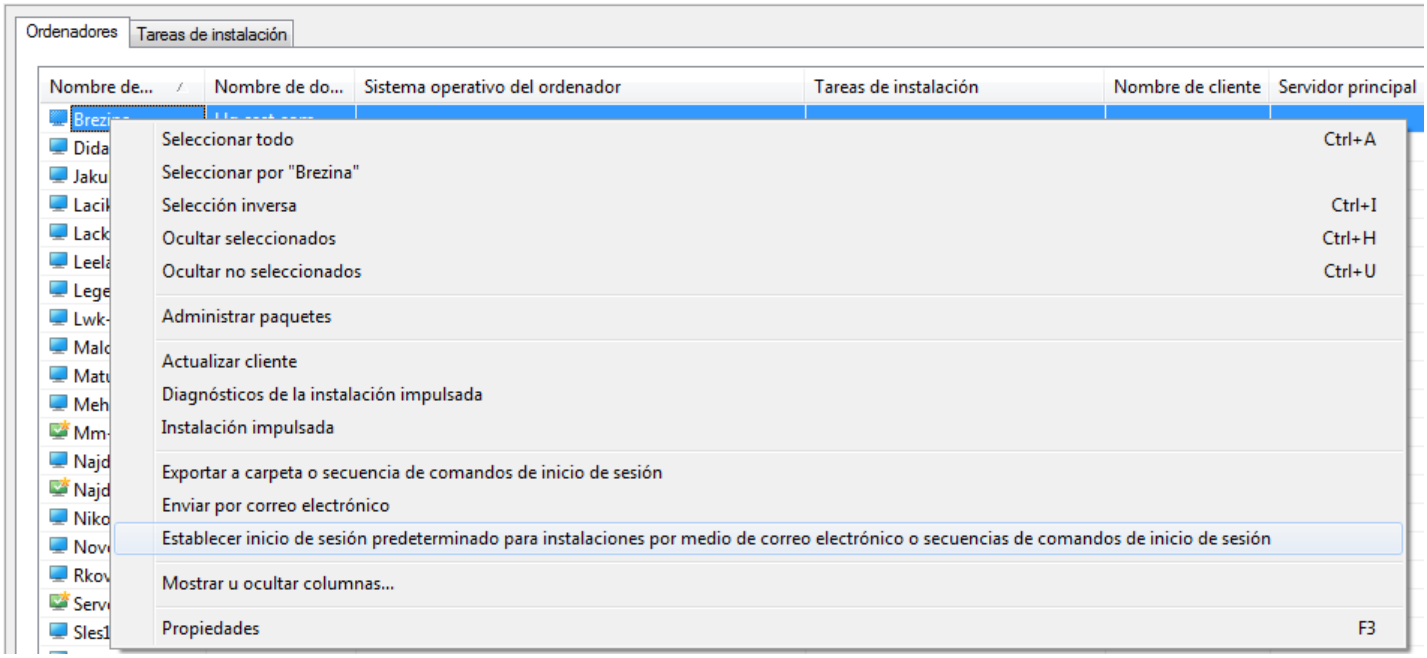
No es necesario utilizar herramientas de ERA para instalar soluciones cliente de ESET. En última instancia, el aspecto más importante es entregar y ejecutar el archivo *einstaller.exe* en las estaciones de trabajo cliente.

Para que *einstaller.exe* se inicie, no es necesario que el usuario registrado actualmente sea un administrador. El agente adopta el nombre de usuario/contraseña/dominio de administrador necesario 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 **Ordenadores** (en la ficha **Instalación remota**), haga clic con el botón derecho del ratón en cualquier punto y seleccione **Exportar a carpeta o script de inicio de sesión** en el menú contextual; a continuación, seleccione el **Tipo** y el nombre del **Paquete** que desea instalar.
- Haga clic en el botón **...** situado junto a **Carpeta** y seleccione el directorio al que se exportará *einstaller.exe*.
- 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 con el parámetro */qn* (versión s 4.x, 3.x) o */silentmode* (versión 2.x). Estos parámetros ejecutarán la instalación sin mostrar ninguna interfaz de usuario.



El nombre de usuario y la contraseña de la cuenta con la que se va a ejecutar la instalación del paquete deben pertenecer a una cuenta con derechos de administrador o, preferiblemente, una cuenta de administrador de dominio.

Durante el proceso de instalación remota, se vuelve a establecer la conexión con ERAS y el agente (*einstaller.exe*) adopta la configuración de **Establecer inicio de sesión predeterminado para instalaciones por medio de correo electrónico o scripts de inicio de sesión**.

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 a ERAS (puerto TCP 2224).
- ERAS inicia una nueva instalación impulsada (con un agente nuevo) del paquete correspondiente (enviado a través del recurso compartido *admin$*). El agente espera una respuesta de ERAS (y envía el paquete mediante el recurso compartido *admin$*). En caso de que no haya respuesta, el agente intentará descargar el paquete de instalación (a través del puerto TCP/IP 2224). En este caso, el nombre de usuario y la contraseña del administrador especificados en **Instalación remota > Iniciar sesión...**, en ERAS, no se transfieren y el agente intenta instalar el paquete en el usuario actual. En los sistemas operativos Microsoft Windows 9x/Me, no se puede usar el recurso compartido administrativo, por lo que el agente establece automáticamente una conexión TCP/IP directa con el servidor. El nuevo agente inicia entonces la descarga del paquete de ERAS a través del protocolo TCP/IP.

La instalación del paquete se inicia con los parámetros .xml asociados en la cuenta definida en ERAS (opción **Establecer inicio de sesión predeterminado para instalaciones por medio de correo electrónico o scripts de inicio de sesión**).

4.2.6 Actualizar

Este tipo de instalación se dirige a clientes que tienen ESS/EAV versión 4.2 o posterior. Desde la versión 4.2, se ha implementado un nuevo mecanismo de actualización que permite a ERA iniciar el proceso de actualización en el cliente sin necesidad del agente *einstaller.exe*. Este mecanismo funciona de manera similar a la Actualización de componentes del programa (PCU), que actualiza los clientes con una versión más reciente del programa. Recomendamos encarecidamente este tipo de actualización para los clientes de ESS/EAV versión 4.2 o posterior.

NOTA: si se ha definido un archivo de configuración personalizado para el paquete de instalación, este se ignorará durante la actualización.

4.2.7 Cómo evitar instalaciones repetidas

En cuanto el agente completa con éxito el proceso de instalación remota, marca al cliente remoto con un indicador 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

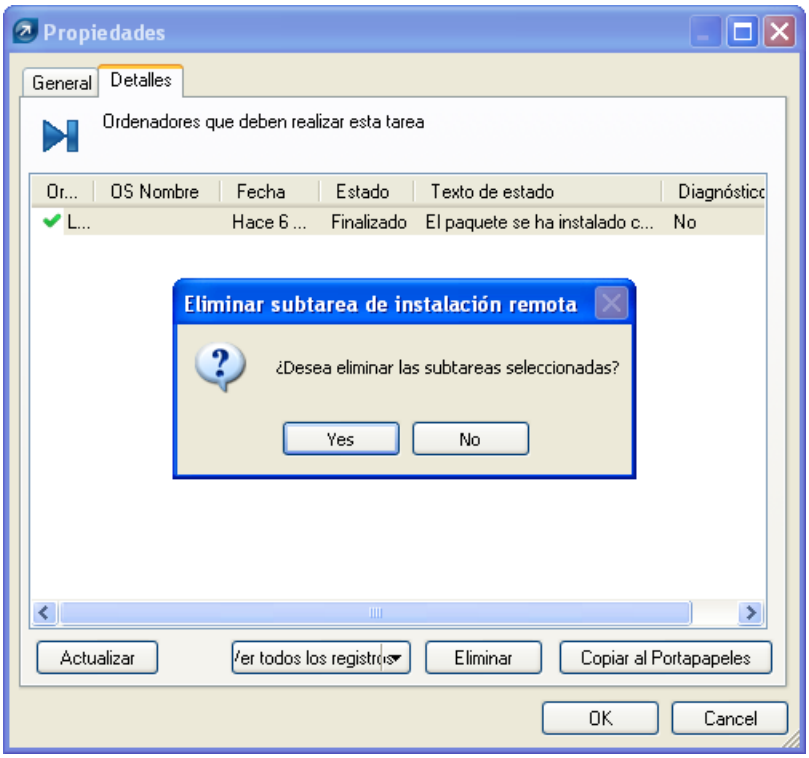
Si el nombre y tipo del paquete definido en el agente *einstaller.exe* coincide con los datos en el registro, la instalación no se realiza. De esta manera, se evita la duplicación de instalaciones en las mismas estaciones de trabajo.

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

ERAS proporciona una característica adicional para evitar las instalaciones repetidas que se activa cuando el instalador vuelve a establecer la conexión con ERAS (TCP 2224). Si se produce un mensaje de error relacionado con la estación de trabajo, o en caso de que la instalación se complete correctamente, se denegarán los intentos de instalación adicionales.

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

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



Para evitar que ERAS deniegue la instalación repetida, elimine las entradas relacionadas en la ficha **Detalles de la tarea de instalación remota**. Para eliminar una entrada, selecciónela, haga clic en el botón **Eliminar** y pulse **Sí** para confirmar.

4.3 Instalación en un entorno empresarial

A la hora de implementar programas en grandes redes, es importante usar una herramienta capacitada para realizar instalaciones de programa remotas en todos los ordenadores 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 todas las estaciones 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 de 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 debe llamarse *cfg.xml*. Para crear un archivo de configuración, se puede utilizar ESET Configuration Editor. Para obtener más información, consulte el capítulo ESET Configuration Editor 32.

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

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

6) Haga clic con el botón derecho del ratón 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_ordenador**ruta**paquete_de_instalación.msi* y haga clic en **Abrir**. No use la opción **Examinar** para localizar el paquete de instalación, ya que 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 todos los ordenadores que entren en el dominio. Para instalar el paquete en los ordenador que están activos actualmente, los usuarios deben cerrar sesión e iniciarla de nuevo.

Si desea que los usuarios tengan 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 ordenadores cliente

5.1 Tareas

Las estaciones de trabajo cliente conectadas a ERAS correctamente y visualizadas en ERAC se pueden configurar y administrar mediante distintos tipos de tareas.

El flujo de trabajo general siguiente se aplica a todas las tareas descritas en los subcapítulos siguientes, salvo en Tarea interactiva 50 (consulte el capítulo para ver una explicación del flujo de trabajo).

Fase I: **Nueva tarea**

Las tareas se pueden aplicar a varios clientes o grupos de clientes.

1) Para aplicar una tarea a una o más estaciones de trabajo cliente, selecciónela y haga clic con el botón derecho en ella en el panel **Clientes**.

2) Haga clic en **Nueva tarea** y seleccione el tipo de tarea que desea realizar.

   NOTA: además, el asistente de tareas se puede abrir desde el menú principal de ERAC haciendo clic en **Acciones > Nueva tarea**.

Fase II: seleccione una de las tareas siguientes:

Tarea de configuración 48
Análisis a petición (desinfección desactivada) 48
Análisis a petición (desinfección activada) 48
Actualizar ahora 49
Tarea Script de SysInspector 49
Tarea Restaurar/eliminar de la cuarentena 49
Generar registro de auditoría de seguridad 50
Mostrar notificación 50

3) Cuando haya seleccionado la tarea deseada, tendrá que realizar las acciones específicas de la tarea que se describen en los diferentes capítulos (consulte los vínculos anteriores).

Fase III: **Seleccionar clientes**

4) En la ventana **Seleccionar clientes**, que se muestra después de configurar la tarea, se pueden modificar las selecciones de cliente. Restrinja la selección mediante la adición de clientes del árbol de información general de clientes **Todos los elementos** (mitad izquierda de la ventana) a la lista **Elementos seleccionados** (mitad derecha de la ventana), o eliminando las entradas de cliente que ya se encuentran en la lista.

   NOTA: haga clic en **Agregar especial...** para abrir una ventana nueva para la adición de clientes del panel **Clientes** o para agregar clientes por **Servidor** y/o **Grupos**.

Fase IV: **Informe de tareas, Finalizar**

5) 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 desinfección si se completan correctamente** elimina todas las tareas entregadas correctamente a las estaciones de trabajo de destino.

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

Los subcapítulos siguientes desarrollan los tipos individuales de tareas para estaciones de trabajo cliente. Cada tipo se acompaña 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 ESET Configuration Editor o exportados desde los clientes también son compatibles con las tareas de configuración. El ejemplo siguiente muestra cómo crear una tarea de configuración que modifique el nombre de usuario y la contraseña en ordenadores de destino. Los modificadores y las opciones no utilizados en este ejemplo se incluyen al final del capítulo.

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

1) Haga clic con el botón derecho del ratón en cualquiera de las estaciones de trabajo marcadas y seleccione **Nueva tarea** > **Tarea de configuración** en 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 ESET Configuration Editor y especifique la configuración que se va a aplicar. Vaya a **ESET Smart Security**, **ESET NOD32 Antivirus** > **Módulo de actualización** > **Perfil** > **Configuración** > **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) Si ya dispone 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 necesarios.

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

8) Haga clic en **Siguiente** para ir a la ventana **Seleccionar clientes**, en la que se mostrarán las estaciones de trabajo a las que se entregará la tarea. En este paso, puede agregar más clientes (o 2 de grupos o servidores seleccionados). Haga clic en **Siguiente** para ir al próximo 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 desinfección si se completan correctamente** elimina todas las tareas entregadas correctamente a las estaciones de trabajo de destino.

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

5.1.2 Tarea Análisis a petición

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

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

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

   NOTA: la opción **Excluir esta sección del análisis a petición** desactiva todas las opciones de la ventana para el tipo de producto seleccionado, que 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 el producto especificado se eliminarán de la lista de destinatarios. Si el administrador marca a los clientes como receptores y excluye el producto mediante el parámetro mencionado anteriormente, la tarea generará un error y se enviará una notificación para indicar que la tarea no se ha podido aplicar. Para evitarlo, el administrador debe especificar siempre los clientes a los que se

asignará la tarea.

2) En **Nombre del perfil** puede seleccionar el perfil de análisis que se aplicará a la tarea.

3) En la sección **Unidades para analizar**, seleccione los tipos de unidad que se deben analizar en los ordenadores cliente. Si la selección es demasiado general, puede 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**. Seleccione **Borrar historial** para restaurar la lista original de unidades para analizar.

4) Haga clic en **Siguiente** para ir a las ventanas de diálogo **Seleccionar clientes** e **Informe de tareas**, que se describen detalladamente en el capítulo Tareas 47.

5) Una vez que la tarea se haya ejecutado en las estaciones de trabajo cliente, los resultados se devuelven a ERAS y se pueden ver en ERAC, 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).

1) Haga clic con el botón derecho del ratón en cualquier estación de trabajo del panel **Clientes** y seleccione **Nueva tarea** > **Actualizar ahora**.

2) Si desea excluir determinados tipos de producto 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**.

3) Para utilizar un perfil de actualización específico en la tarea **Actualizar ahora**, active la opción **Especificar nombre de perfil** y seleccione el perfil deseado. También puede seleccionar **Nombre de perfil definido por el usuario** e introducir el nombre del perfil. Al hacer clic en **Borrar historial**, el valor del campo volverá al valor predeterminado.

4) A continuación, haga clic en **Siguiente** para ir a las ventanas de diálogo**Seleccionar clientes** e **Informe de tareas**. Para ver una descripción de estos cuadros de diálogo, consulte el capítulo Tareas 47.

5.1.4 Tarea Script de SysInspector

La tarea Script de SysInspector le permite ejecutar scripts en ordenadores de destino. Sirve para eliminar objetos no deseados del sistema. Para obtener más información, consulte la página de ayuda de ESET SysInspector 98.

1) Cuando haya finalizado las Fases I y II que se describen en el capítulo Tareas 47, haga clic en **Seleccionar** para elegir el script que dese ejecuta en la estación de trabajo de destino.

2) Haga clic en **Ver y modificar** para ajustar el script.

3) Haga clic en **Siguiente** para ir a las ventanas de diálogo **Seleccionar clientes** e **Informe de tareas**, que se describen detalladamente en el capítulo Tareas 47.

4) 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**.

NOTA: las tareas de script de SysInspector sólo se admiten en ESET Smart Security/ESET NOD32 Antivirus versión 4.0 y posteriores.

5.1.5 Tarea Restaurar/eliminar de la cuarentena

Esta tarea le permite restaurar o eliminar los objetos en cuarentena especificados de la cuarentena del cliente.

1) Con la ventana **Restaurar/eliminar de la cuarentena** abierta (consulte el capítulo Tareas 47), haga clic en el botón de opción **Restaurar/Eliminar**, según el tipo de acción que desee realizar sobre el objeto en cuarentena.

   NOTA: si se restaura un objeto en cuarentena que aún se detecta como una amenaza, es recomendable seleccionar la opción **Agregar también las exclusiones**; si no se hace, el antivirus podría detener la acción o devolver el objeto a la cuarentena.

2) Seleccione una condición para especificar los objetos en cuarentena que desea restaurar o eliminar y haga clic en Siguiente.

NOTA: si ha hecho clic con el botón derecho del ratón sobre una entrada de cuarentena directamente en la ficha Cuarentena (y ha seleccionado la opción **Tarea Restaurar/eliminar de la cuarentena**) para abrir la ventana Restaurar/eliminar de la cuarentena, no es necesario que especifique ninguna condición (se seleccionará automáticamente la opción **Por hash** y se utilizará como identificador el código hash del archivo en cuarentena).

3) Seleccione los clientes para la operación de restauración o eliminación (consulte el capítulo Tareas 47) y haga clic en **Siguiente**.

4) Revise la configuración en la ventana **Informe de tareas**, asigne un nombre a la tarea, especifique la hora a la que desea aplicar la tarea y las opciones de desinfección, si lo desea; a continuación, haga clic en **Finalizar** para confirmar. Consulte el capítulo Tareas 47 para obtener más detalles.

5.1.6 Tarea Generar registro de auditoría de seguridad

Esta tarea se aplica únicamente a ESET Mobile Security.

Comprobaciones de la auditoría de seguridad: nivel de batería, estado de Bluetooth, espacio libre en disco, visibilidad del dispositivo, red doméstica y procesos en ejecución. Se generará un informe detallado, donde se indicará si el valor del elemento se encuentra por debajo del umbral especificado o si podría representar un riesgo de seguridad (p. ej., visibilidad del dispositivo activada, etc.).

Para ejecutar la auditoría de seguridad en el teléfono:
1) Haga clic con el botón derecho del ratón en el nombre del cliente, en el panel **Clientes** y seleccione **Nueva tarea** > **Generar registro de auditoría de seguridad** en el menú contextual.
2) Haga clic en **Siguiente** para ir a las ventanas **Seleccionar clientes** e **Informe de tareas**. Para ver una descripción de estas ventanas, consulte el capítulo Tareas 47.

5.1.7 Tarea Mostrar notificación

Esta tarea se aplica únicamente a ESET Mobile Security.

Para enviar una notificación (p.ej., un mensaje de alerta) al teléfono:
1) Haga clic con el botón derecho del ratón en el nombre del cliente, en el panel **Clientes** y seleccione **Nueva tarea** > **Mostrar notificación** en el menú contextual.
2) Escriba el **Título** de la notificación y el **Cuerpo** del mensaje en los campos correspondientes y seleccione el **Nivel de detalle** de la notificación.
3) Haga clic en **Siguiente** para ir a las ventanas **Seleccionar clientes** e **Informe de tareas**. Para ver una descripción de estas ventanas, consulte el capítulo Tareas 47.

5.1.8 Tarea interactiva

Esta tarea se diferencia de las demás tareas aquí descritas en su ejecución y aplicación.

En la ficha **Clientes**, se puede ver la columna **Texto de estado de la protección**, que controla el estado de la protección de todos los clientes de ESET conectados. Un campo en blanco indica que el estado de la protección de un cliente específico se encuentra en el nivel **Máxima protección**. Si el nivel de protección de un cliente es inferior al máximo, se mostrará una alerta de estado de la protección de color rojo o naranja en el **Texto de estado de la protección** (p.ej., **El cortafuegos personal de ESET está desactivado**).

ERA permite al administrador manipular estos ajustes en la ficha **Clientes**, tal como se indica a continuación:

1) Haga doble clic en una entrada de cliente relevante de la ficha **Cliente**.

2) En la ventana **Propiedades**, haga clic en la ficha **Estado de la protección**.

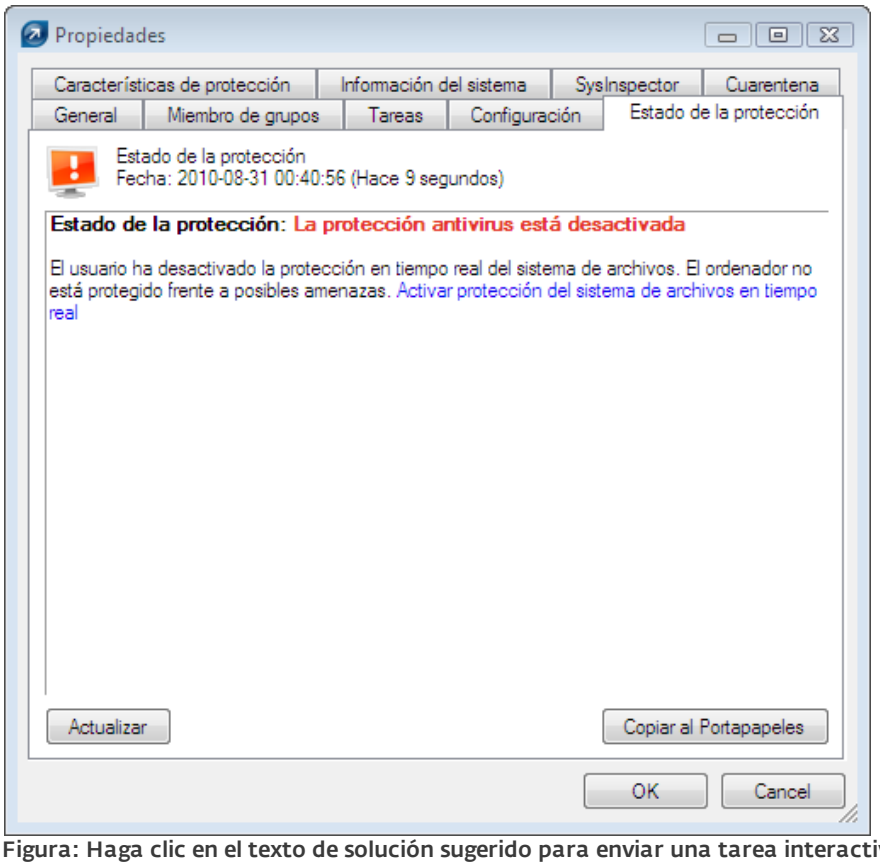


Figura: Haga clic en el texto de solución sugerido para enviar una tarea interactiva al cliente.

3) El campo **Estado de la protección** contendrá una o más alertas. Haga clic en el texto azul que sugiere una solución al final de cada mensaje.

4) Haga clic en **Sí** para confirmar la ejecución de la tarea interactiva.

5) Cuando haya repetido los pasos 3 y 4 para todos los mensajes mostrados, haga clic en **Actualizar** varias veces para ver si los mensajes de estado desaparecen.

Cuando haya solucionado todos los problemas, el mensaje de estado de la protección cambiará a **Estado de la protección: El sistema está protegido**.

NOTA: la característica de tarea interactiva es compatible con ESET Smart Security/ESET NOD32 versión 3 y versiones posteriores.

5.2 Administrador de grupos

El Administrador de grupos es una herramienta potente para la administración de clientes, ya que los divide en diferentes grupos y les aplica diferentes configuraciones, tareas, restricciones, etc. Se puede acceder fácilmente a ella a través de **Herramientas > Administrador de grupos** o **CTRL+G**. Los grupos son independientes de cada ERAS y no se replican.
Puede crear sus propios grupos en función de las necesidades de su red empresarial, o simplemente sincronizar grupos de clientes de ERAC con Microsoft Active Directory, con el comodín de **Sincronización de Active Directory** de la ventana del Administrador de grupos.

Hay dos tipos principales de grupos de cliente:
- Grupos estáticos
- Grupos paramétricos

Tanto los grupos estáticos como los grupos paramétricos se pueden utilizar en varios sitios de ERA, lo que mejora considerablemente las funciones de administración de clientes.

5.2.1 Grupos estáticos

Los grupos estáticos se crean para separar los clientes de la red en grupos y subgrupos con nombres; es decir puede crear un grupo Marketing que contenga todos los clientes de marketing y crear subgrupos especializados como, por ejemplo, Ventas locales, Administración de EMEA, etc.

La ventana principal Grupos estáticos se divide en dos partes. En el lado izquierdo se muestran, jerárquicamente, los grupos y subgrupos existentes. Los clientes incluidos en el grupo seleccionado se enumeran en el lado derecho de la ventana. De forma predeterminada, sólo se muestran los clientes del grupo seleccionado. Si desea ver los clientes incluidos en los subgrupos del grupo seleccionado actualmente, marque la casilla de verificación **Mostrar clientes en subgrupos** en el lado derecho de la ventana.

Para crear un grupo nuevo, haga clic en **Crear** y seleccione un nombre para él. El grupo nuevo se creará como un subgrupo del grupo principal seleccionado actualmente. Si desea crear un grupo principal, seleccione la raíz del árbol jerárquico de **Grupos estáticos**. En el campo Grupo principal se especifica el nombre del grupo principal del grupo que se acaba de crear (es decir, "/" para la raíz). Le recomendamos que utilice un nombre que indique dónde están ubicados los ordenadores (p. ej., *Departamento financiero*, *Asistencia técnica*, etc.). El campo Descripción se puede usar para dar una descripción más detallada del grupo (p. ej., *"Ordenadores 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.

NOTA: cuando se envíe una tarea al grupo principal, todas las estaciones que pertenezcan a sus subgrupos también aceptarán esta tarea.

También se pueden crear grupos vacíos para utilizarlos más adelante.

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**; 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 el botón **Agregar especial...** para ver más opciones.

Seleccione la opción **Agregar clientes cargados en el panel de clientes** para agregar todos los clientes mostrados en la sección de clientes, o bien seleccione la opción **Sólo seleccionados**. Para agregar clientes que ya pertenecen a otro servidor u otro grupo, selecciónelos en las listas de la derecha y la 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 administrador de grupos estáticos. El nuevo grupo debería aparecer junto 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. Pulse el botón **Actualizar** para actualizar los clientes del grupo.

También puede **Importar/Exportar** los clientes del grupo seleccionado actualmente a un archivo *.xml*.

5.2.2 Grupos paramétricos

Los grupos paramétricos, además de los estáticos, pueden resultar muy útiles. Las estaciones cliente se asignan dinámicamente a un grupo paramétrico determinado cuando se cumplen las condiciones del grupo. La ventaja de los grupos paramétricos es la capacidad de usarlos en varios sitios, incluidos filtros, directivas, informes y notificaciones.

La ventana principal Grupos paramétricos consta de cuatro secciones. En **Grupos paramétricos** se enumeran los grupos principales y los subgrupos que se crearon. Cuando haya seleccionado un grupo determinado de grupos paramétricos, los clientes que pertenezcan al grupo seleccionado se enumerarán en la sección **Grupo seleccionado**. **NOTA:** cuando se selecciona un grupo principal, la lista también contendrá miembros del subgrupo.

Los parámetros establecidos para un grupo seleccionado se especifican en la sección **Parámetros** de la ventana. Los parámetros se pueden modificar o agregar en cualquier momento con el botón **Modificar...**

En la sección **Estado de sincronización** se muestra una barra de progreso para el proceso de sincronización.

Para crear un grupo nuevo, haga clic en el botón **Crear...** El nuevo grupo se creará como un subgrupo del grupo principal seleccionado actualmente. Si desea crear un grupo principal, seleccione la raíz del árbol jerárquico de **Grupos paramétricos**. En el campo Grupo principal se especifica el nombre del grupo principal del grupo que se acaba de crear (es decir, "/" para la raíz). Introduzca el **nombre** y una breve **descripción** del nuevo grupo. El próximo paso consiste en la creación de **Parámetros del filtro de clientes**, que se puede realizar seleccionando las opciones tras pulsar el botón **Modificar...**. Si activa la casilla de verificación **Permanente**, los clientes se agregarán automáticamente a este grupo cuando cumplan las condiciones, pero no se quitarán nunca. El contenido de un grupo permanente se puede restablecer manualmente desde la raíz.

NOTA: este parámetro sólo se puede establecer cuando se crea un grupo nuevo.

Para modificar un grupo existente, sólo tiene que seleccionarlo en la lista Grupos paramétricos y, a continuación, pulsar el botón **Modificar...** situado en la parte inferior de la ventana. Para eliminar un grupo, selecciónelo y pulse el botón **Eliminar**.
La lista de grupos se puede actualizar manualmente con el botón **Actualizar**. Para importar un grupo desde un archivo, selecciónelo en la sección **Grupos paramétricos** en la que desea importarlo y haga clic en el botón **Importar...** Haga clic en **Sí** para confirmar la selección. Localice el archivo que desea importar y haga clic en **Abrir**. El grupo (y todos sus subgrupos) se importarán en la ubicación seleccionada. Para exportar un grupo (y todos sus subgrupos), selecciónelo en la sección **Grupos paramétricos**, haga clic en la flecha del botón **Importar...** y seleccione **Exportar...** Haga clic en **Sí** para confirmar, seleccione un nombre y una ubicación para el archivo de exportación y, a continuación, haga clic en **Guardar**.

NOTA: puede utilizar el ratón para arrastrar y soltar grupos que ya se encuentran en la sección **Grupos paramétricos**.

5.2.3 Sincronización de Active Directory

La Sincronización de Active Directory utiliza la creación de grupos automáticos (con los clientes correspondientes) basada en la estructura definida por Active Directory. Esta función permite al administrador clasificar los clientes en grupos, siempre que el nombre del cliente coincida con el tipo de objeto *ordenador* en el lado de Active Directory (AD) y pertenezca a grupos de AD.

Hay dos opciones principales que determinan la forma de sincronización:

La opción **Sincronizar grupos** le permite seleccionar los grupos de AD que se sincronizarán. La opción **Todos los grupos** tiene como resultado la sincronización de la estructura completa del árbol de AD, independientemente de si los grupos de AD contienen clientes de ERA o no. Las dos opciones siguientes (**Sólo los grupos que contienen clientes del ERA Server** y **Sólo los grupos que contienen clientes principales del servidor ERA**) suponen una sincronización más estricta y sincronizan únicamente los grupos que contienen clientes actuales de ERA.

La opción **Tipo de sincronización** le permite definir si los grupos de AD que se sincronicen se agregarán a los grupos existentes de AD (**Importación de grupos de AD**) o si los grupos actuales de AD se sustituirán completamente por los que se van a sincronizar (**Sincronización de grupos de AD**).

La opción **Sincronizar** le permite programar la sincronización de AD con un intervalo de tiempo determinado.

La sincronización de Active Directory se puede configurar detalladamente con Configuration Editor (**ESET Remote Administrator** > **ERA Server** > **Configuración** > **Grupos** > **Opciones de sincronización de Active Directory**). De forma predeterminada, sólo se sincronizan los **Grupos de seguridad de los sistemas y las Unidades de organización de los sistemas**. Sin embargo, puede marcar la opción deseada para agregar otros objetos de Active Directory.

NOTA: para que ERAS se sincronice con Active Directory, no es necesario que esté instalado en el controlador de dominio. El único requisito es que sea posible acceder al controlador de dominio desde el ordenador en el que esté ubicado ERAS. Para configurar la autenticación para el controlador de dominio, vaya a **Herramientas** > **Opciones del servidor** > **Avanzadas** > **Modificar configuración avanzada** > **ESET Remote Administrator** > **ERA Server** > **Configuración** > **Active Directory**. El formato del nombre del servidor es *LDAP://nombredeservidor* o *GC://nombredeservidor*. Si está vacío, se utiliza un catálogo global (GC).

5.3 Directivas

Las directivas se parecen en muchos aspectos a las tareas de configuración, exceptuando que no se trata de tareas puntuales enviadas a una o más estaciones de trabajo. Las directivas 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 un cliente está obligado a adoptar.

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 se divide en cuatro secciones: **Configuración de directivas**, **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 directivas de ERAS. ERAS puede utilizar múltiples directivas, que heredan parámetros las unas de las otras, 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 mediante herencia se denominan *directivas combinadas*. La herencia se basa en el principio principal - secundario; es decir, 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 ESET Configuration Editor; haga clic en **Modificar** y defina los parámetros para el producto (o cliente) de seguridad de ESET seleccionado. 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 ordenadores de destino. Se aplica el mismo principio a las directivas heredadas y combinadas; una directiva secundaria adoptará sólo parámetros activos de una directiva principal.

Los ERA Server admiten varias directivas (**Agregar nueva directiva secundaria**). Las opciones siguientes 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 ERAC. Para crear una directiva en un servidor inferior debe conectarse directamente a este último.

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

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 (aunque esté 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 tienen 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.

Las directivas también se pueden importar o exportar desde/en un archivo *.xml*, o importar desde grupos. Para obtener más información, consulte el capítulo titulado Importación/exportación de directivas 57.

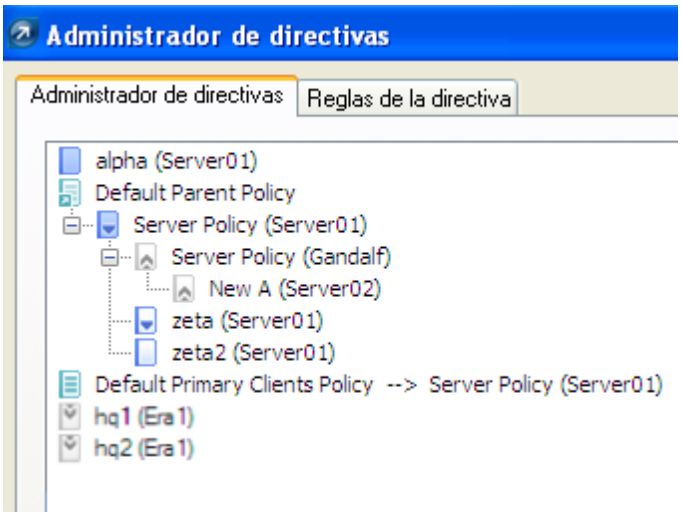
5.3.3 Directivas virtuales

Además de las directivas creadas, así como las replicadas desde otros servidores (consulte el capítulo Ficha Replicación 82), el árbol de directivas contiene también 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) desde ERAS en cuestión, a no ser que ya hayan adoptado otra directiva de las Reglas de la directiva (para obtener más información, consulte el capítulo Asignación de directivas a clientes 57). Las directivas virtuales son vínculos a otras directivas ubicadas en el mismo servidor.

5.3.4 Función y objetivo de las directivas en la estructura de árbol de directivas



A todas las directivas del árbol de directivas se les asigna un icono, que se sitúa 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: la directiva se creó 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 se pueden aplicar dentro del servidor, a clientes conectados al servidor. También puede funcionar como directiva principal de otra directiva del mismo servidor.

Iconos con destinos azules: la directiva también se creó en el servidor, aunque se seleccionó la opción **Anular directivas secundarias** (para obtener más información, consulte el capítulo Cómo crear directivas 54).

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 se pueden ver o eliminar 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. Se pueden utilizar como directivas principales para otras directivas, asignar a clientes (**Agregar clientes**) o eliminar (**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 soltarla con el ratón.

Las reglas de directiva existentes se pueden importar o exportar desde/a un archivo *.xml* mediante el botón **Importar.../Exportar...** En la importación, los conflictos de nombre (la directiva existente y la directiva importada tienen el mismo nombre) se solucionan agregando una cadena aleatoria al final del nombre de la directiva importada.

5.3.5 Visualización de directivas

Las directivas del árbol de directivas se pueden ver directamente en Configuration Editor, haciendo clic en **Ver...** o **Ver combinadas...**

Ver combinadas: muestra la directiva combinada creada por herencia (el proceso de herencia se aplica a la configuración de la directiva principal). Esta opción se visualiza de forma predeterminada, ya que la directiva actual ya es una directiva combinada.

Ver: muestra la directiva original antes de su combinación con una directiva principal.

En los servidores inferiores, están disponibles las siguientes opciones para directivas heredadas de servidores superiores:

Ver combinadas: ver anterior.

Ver la parte de anulación: este botón se aplica a las directivas que tienen el atributo Anular directivas secundarias. Esta opción sólo muestra la parte forzada de la directiva, es decir, la que tiene prioridad sobre las demás opciones de las directivas secundarias.

Ver parte no forzada: tiene el efecto opuesto a Ver la parte de anulación, sólo muestra los elementos activos que no tienen el atributo Anular...

5.3.6 Importación/exportación de directivas

El Administrador de directivas le permite importar y exportar directivas y reglas de directiva. Las directivas existentes se pueden importar o exportar desde/a un archivo *.xml* mediante el botón **Importar directivas.../Exportar directivas...** Además, las directivas se pueden importar desde grupos mediante el botón **Importar desde grupos...**. Para importar y exportar reglas de directiva, haga clic en el botón **Importar.../Exportar...** También puede crear reglas con el **Asistente de reglas de directiva**.

En la importación, los conflictos de nombre (la directiva existente y la directiva importada tienen el mismo nombre) se solucionan agregando una cadena aleatoria al final del nombre de la directiva importada. Si un conflicto no se puede resolver de esta manera (normalmente porque el nombre nuevo es demasiado largo), la importación termina con la alerta *Conflicto de nombre de directiva no resuelto*. La solución consiste en eliminar o cambiar el nombre de las directivas o reglas de directiva que entran en conflicto.

5.3.7 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 dicho servidor con 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.

5.3.7.1 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 en Configuración global de directivas. Esta directiva se aplica a los clientes principales, es decir, a los clientes que se conectan a ERAS directamente. Para obtener más información, consulte el capítulo Directivas virtuales 55.

5.3.7.2 Asignación manual

Hay dos maneras de asignar directivas manualmente: Haga clic con el botón derecho del ratón en el panel **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 la opción **Bajar directiva replicable** está seleccionada, la ventana también mostrará los clientes replicados desde servidores inferiores. Seleccione los clientes que recibirán la directiva mediante el método de arrastrar y soltar, o haciendo clic en **>>** para moverlos a **Elementos seleccionados**. Los clientes recién 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 los clientes seleccionados o agregar clientes de servidores o grupos seleccionados.

5.3.7.3 Reglas de la directiva

La herramienta **Reglas de la directiva** permite que un administrador asigne directivas automáticamente a estaciones de trabajo de una manera más exhaustiva. Las reglas se aplican inmediatamente después de que el cliente se conecte al servidor; además, 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, tendrá prioridad la configuración que imponen las reglas de la directiva.

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 un **Nombre**, **Descripción**, **Parámetros del filtro de clientes** y **Directiva** (una directiva que se aplicará a todos los clientes que cumplan con los criterios especificados).

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

Los criterios disponibles son:

(NO) DESDE el servidor principal: si (no) se encuentra en el servidor principal.
(NO) ES un cliente nuevo: si (no) es un cliente nuevo.
(NO) TIENE Indicador "Nuevo": se aplica a los clientes con/sin el indicador Cliente nuevo.
Servidor principal (NO) EN (especificar): si el nombre del servidor 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 ordenador (especificar): si el nombre del ordenador es...
TIENE Máscara IP (especificar): si el cliente pertenece al grupo definido por la máscara y la dirección IP...
TIENE Rango de IP (especificar): si el cliente pertenece al grupo definido por el rango de IP...
(NO) TIENE Directiva definida (especificar): si el cliente adopta (o no) la directiva...
Nombre de producto (NO) EN: si el nombre de producto es...
(NO) ES la versión de producto: si la versión del producto es...
Máscara de información personalizada del cliente (NO) EN: si la información personalizada del cliente contiene...
(NO) TIENE Estado de protección (especificar): si el estado de protección del cliente es...
(NO) ES la versión de la base de firmas de virus: si la base de firmas de virus es...
La última conexión (NO) ES anterior a (especificar): si la última conexión es anterior a...
(NO) Esperando para reiniciar: el cliente está esperando para reiniciarse.

Las reglas de la directiva se puede importar o exportar desde/en un archivo *.xml*; además, se pueden crear automáticamente con el **Asistente de reglas de directiva**, lo que le permite crear una estructura de directiva basada en la estructura de grupo existente y asignar las directivas creadas a grupos mediante la creación de las reglas de directiva correspondientes. Para obtener más información sobre la importación y exportación de reglas de directiva, consulte el

capítulo titulado Importación/exportación de directivas 57.

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

5.3.8 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 ERAC.

NOTA: una directiva podría estar vinculada a otros servidores o directivas (como una directiva principal, como una directiva principal para servidores inferiores, como una directiva predeterminada para clientes principales, 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 disponibles o no, 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 los clientes principales, para reemplazar a la que está eliminando. Los clientes principales pueden adoptar la **Directiva predeterminada para clientes principales**, así como otras directivas del mismo servidor (asignado manualmente con **Agregar clientes** o forzado con **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 el indicador 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, aunque 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 sirve como una directiva virtual (consulte la sección **Configuración global de directivas**), se debe sustituir por otra (para obtener más información, consulte el capítulo Directivas virtuales 55). Para la sustitución puede usar cualquier directiva del servidor en cuestión, o bien el indicador N/D.

Nueva directiva predeterminada para clientes principales: si la directiva eliminada sirve como una directiva virtual (consulte la sección **Configuración global de directivas**), se debe sustituir por otra (para obtener más información, consulte el capítulo Directivas virtuales 55). Puede usar una directiva del mismo servidor para la sustitución.

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

5.3.9 Configuración especial

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

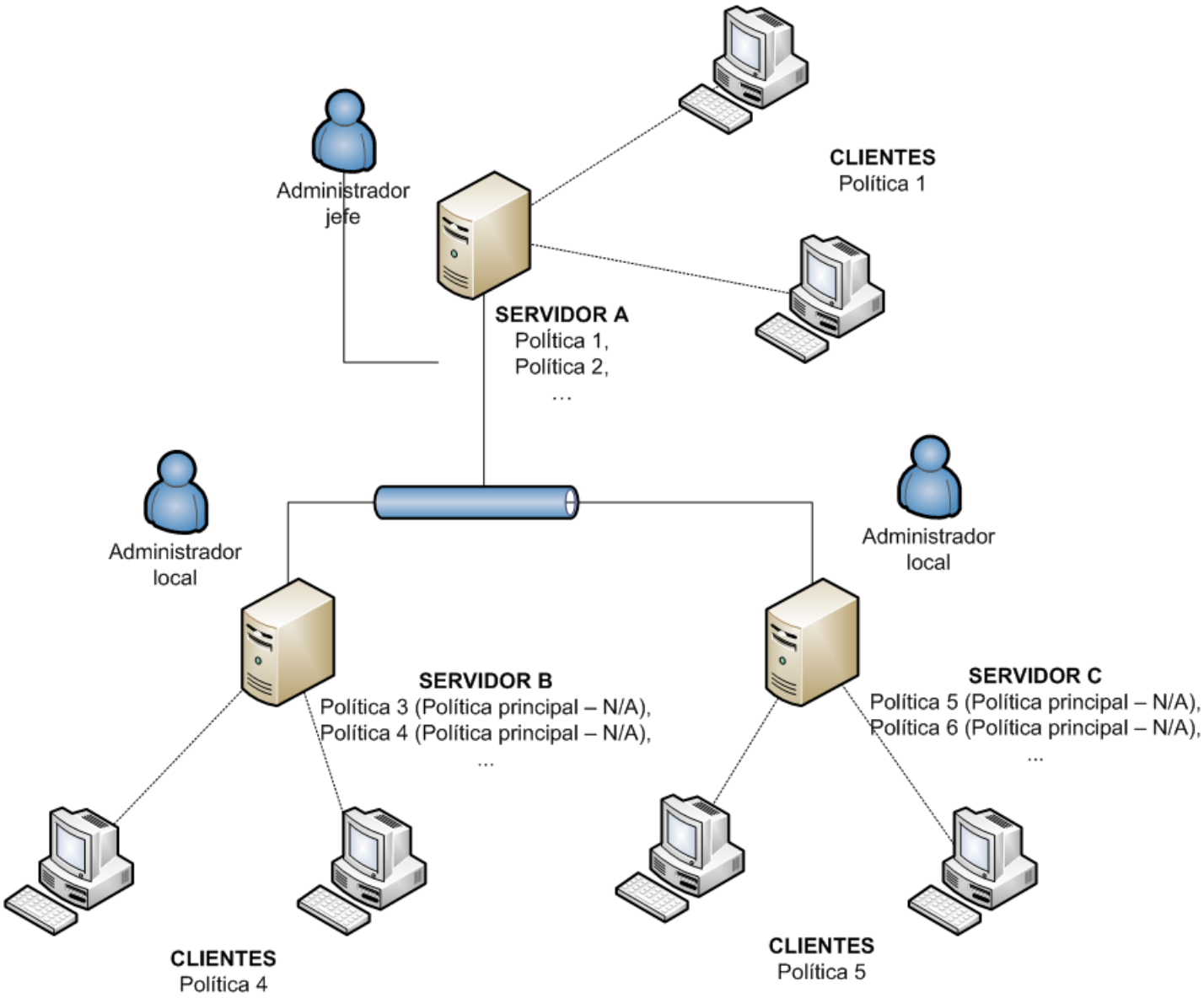
Intervalo de ejecución de directivas (minutos):
Esta característica se aplica a las directivas del intervalo especificado. Recomendamos la configuración predeterminada.

Desactivar el uso de directivas:
Active esta opción para cancelar la aplicación de directivas a los servidores. Recomendamos esta opción si existe algún problema con la directiva. Si no desea aplicar una directiva a algunos clientes, la mejor solución es asignar una directiva vacía.

5.3.10 Situaciones de implementación de directivas

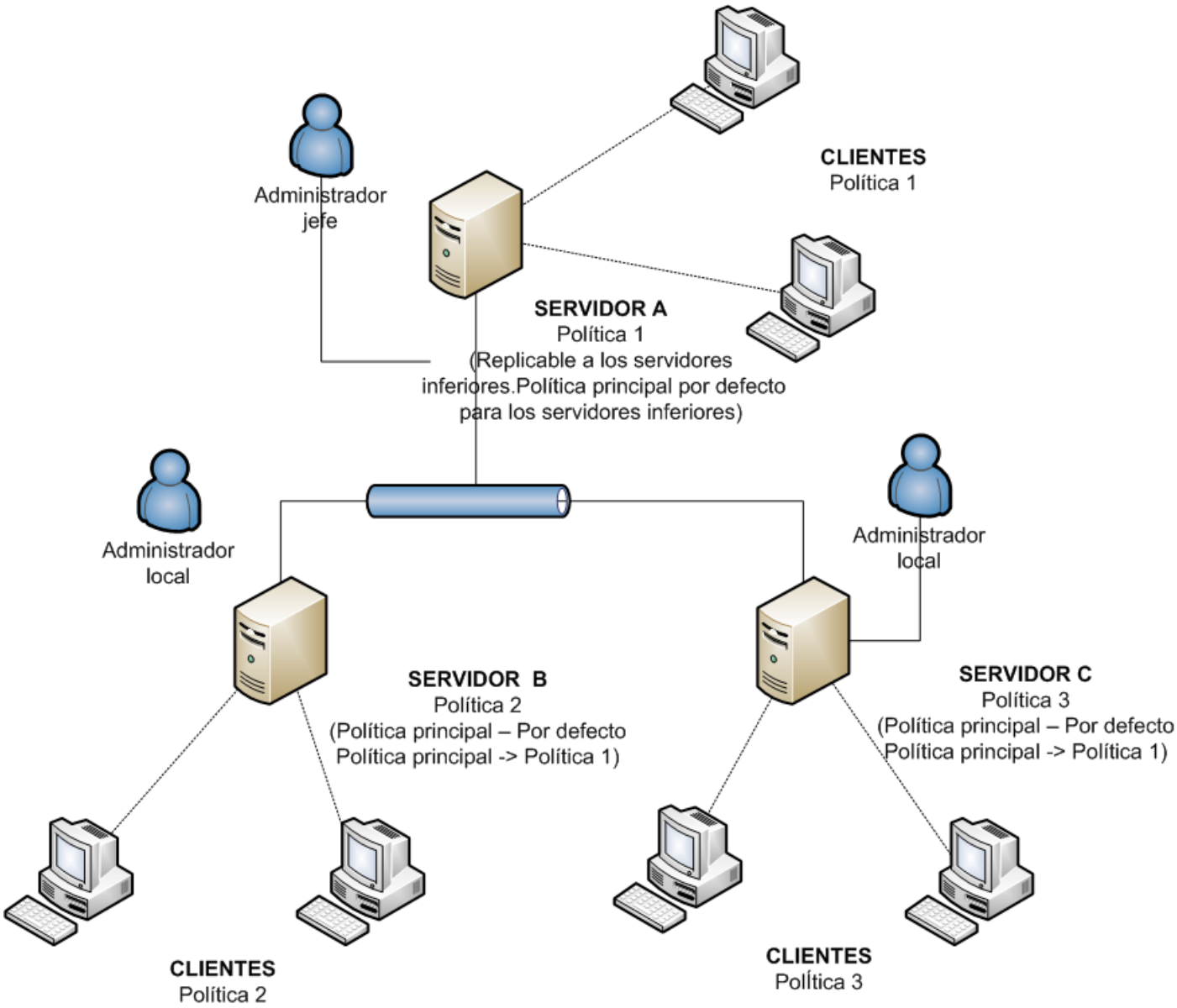
5.3.10.1 Cada servidor es una unidad independiente y las directivas se definen localmente

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 se ha creado al menos una directiva. Los servidores inferiores están ubicados en las sucursales de la empresa. Ambos servidores están gestionados por administradores locales. Cada administrador decide las directivas que se deben asignar a los diferentes clientes de sus servidores. El administrador principal no interviene en las configuraciones que diseñan los administradores locales, y no asigna directivas a los clientes de sus servidores. 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 el indicador 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).



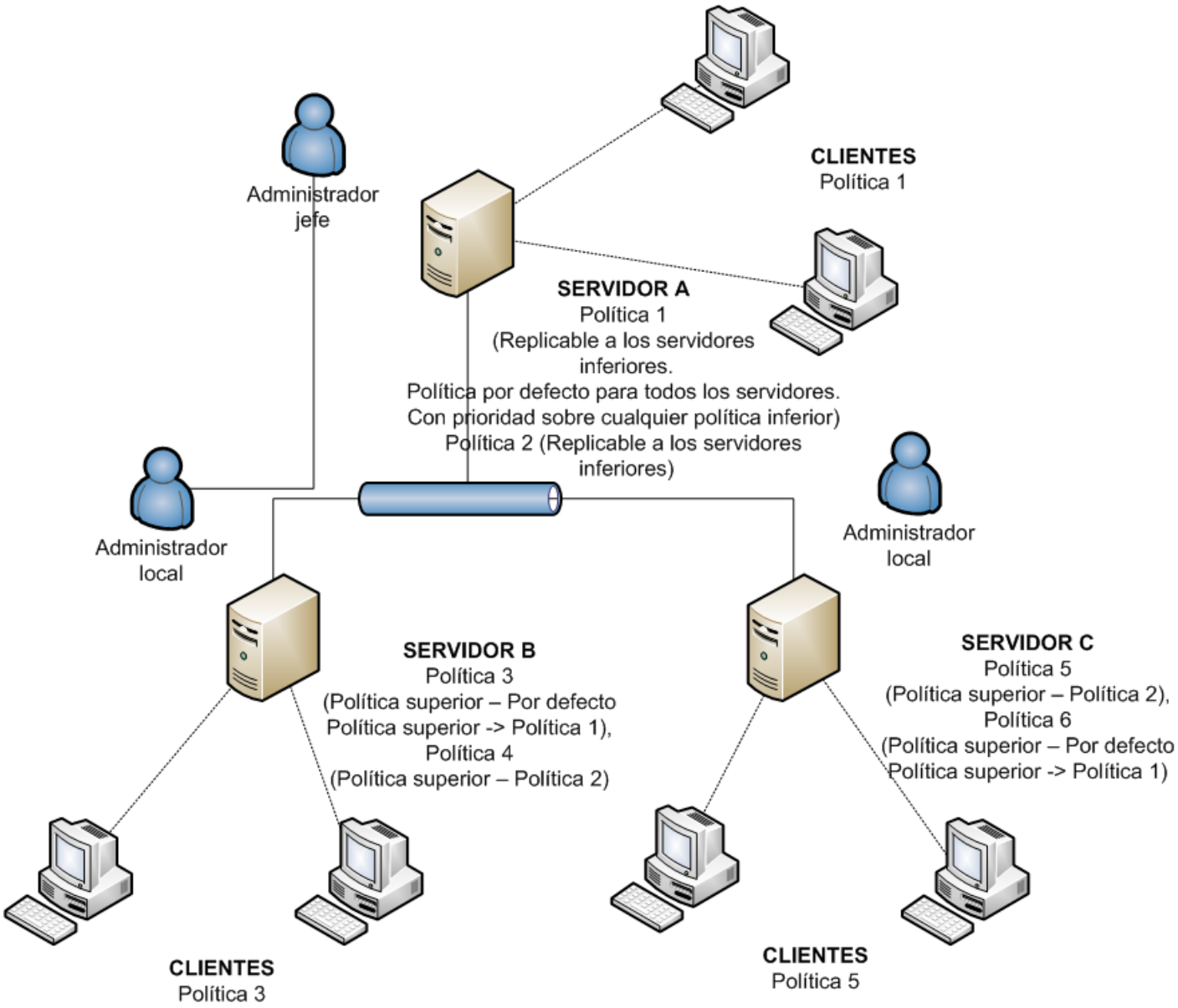
5.3.10.2 Los servidores se administran de forma individual y las directivas se gestionan localmente, pero la Directiva principal predeterminada se hereda del servidor superior

La configuración de la situación anterior también se aplica en este caso. 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. Las Directivas secundarias de los servidores inferiores pueden heredar la Directiva principal predeterminada, mientras que los administradores locales aún pueden modificarla según sus propias directivas.



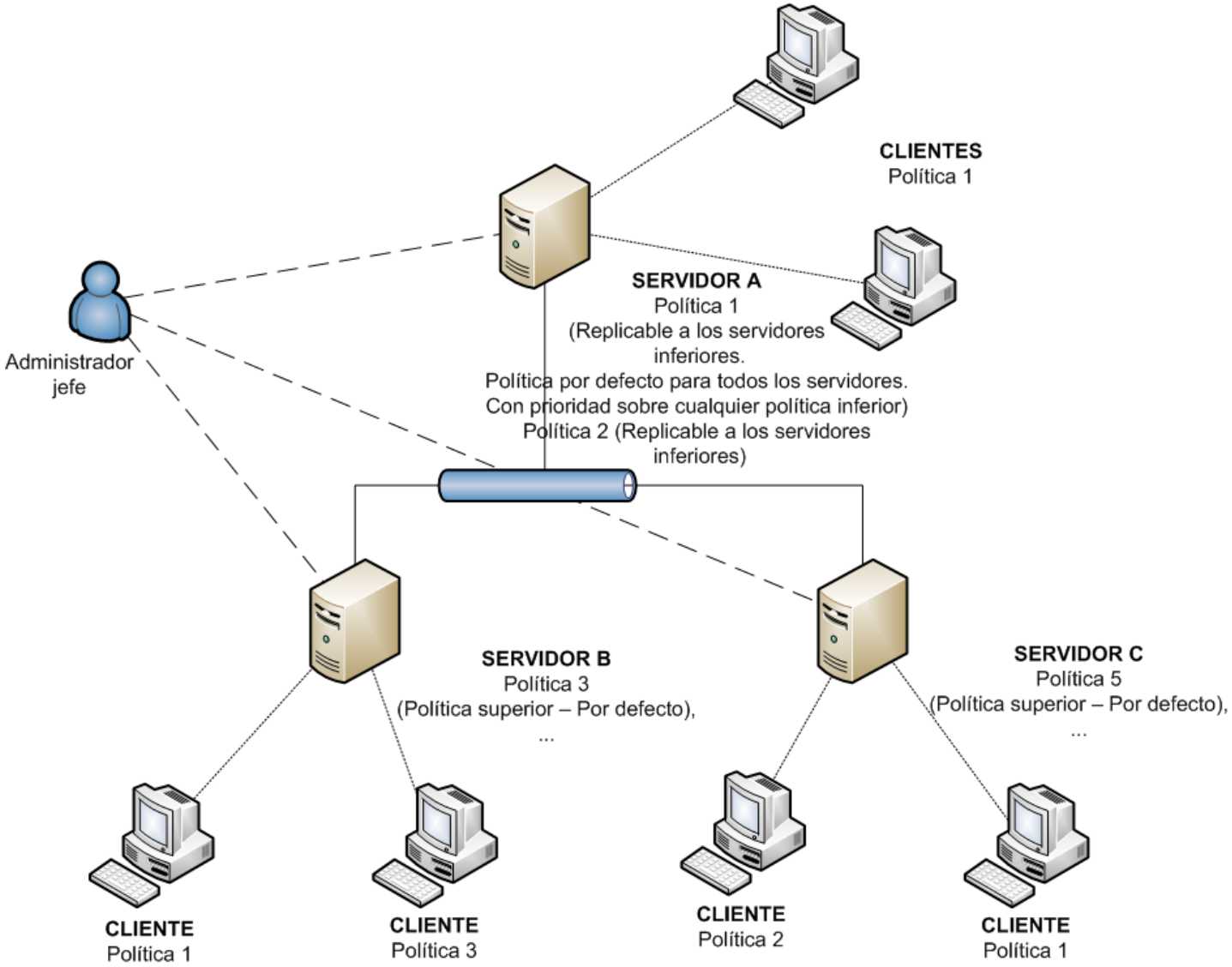
5.3.10.3 Herencia de directivas de un servidor superior

El modelo de red de esta situación es el mismo que en las dos situaciones anteriores. Además, el servidor maestro y la Directiva principal predeterminada contienen 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 siguiente), 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 funcionan como directivas principales para las directivas locales. El atributo **Anular...** establece que las configuraciones de las directivas seleccionadas anulen las establecidas en los servidores locales.



5.3.10.4 Asignación de directivas sólo desde el servidor superior

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



5.3.10.5 Uso de las reglas de la directiva

El ejemplo siguiente incluye la asignación automática de directivas basada en las reglas de directiva. Se trata de un método complementario que se debería usar 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 reglas de directivas, como sucedería si el servidor superior asignase una directiva a clientes basada en las reglas de directiva y 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.

5.3.10.6 Uso de grupos

En algunas situaciones, la asignación de directivas a grupos de clientes puede complementar las situaciones anteriores. Los grupos se pueden crear manualmente o mediante la opción **Sincronización de Active Directory**.
Los clientes se pueden agregar a grupos manual (**Grupos estáticos**) o automáticamente, mediante las propiedades del grupo (**Grupos paramétricos**). Consulte el capítulo Administrador de grupos 51 para obtener más detalles.
Para asignar una directiva a un grupo de clientes, puede utilizar la opción de asignación puntual del **Administrador de directivas** (**Agregar clientes > Agregar especial**) o entregar las directivas automáticamente mediante **Reglas de la directiva**.

A continuación se describe una situación posible:

El administrador desea asignar diferentes políticas a clientes que pertenecen a distintos grupos de AD y modificar la directiva del cliente automáticamente cuando este cambia de grupo.

1) El primer paso consiste en configurar **Sincronización de Active Directory** en el **Administrador de grupos** en función de sus necesidades. Aquí, lo importante es programar correctamente la sincronización de AD (opciones posibles: cada hora, diariamente, semanalmente, mensualmente).
2) Tras la primera sincronización correcta, los grupos de AD aparecen en la sección **Grupos estáticos**.
3) Cree una regla de directiva nueva y marque **Grupos del administrador remoto EN** y/o **Grupos del administrador remoto NO EN** como condición de la regla.
4) Especifique los grupos de AD que desea agregar a la condición.
5) En el paso siguiente, defina la directiva que se aplicará a los clientes que cumplan las condiciones de la regla y pulse **Aceptar** para guardar la regla.

NOTA: Los pasos del 3 al 5 se pueden omitir si se utiliza el **asistente de reglas de directiva**, que le permite crear una estructura de directiva basada en la estructura de grupo existente y asignar las directivas creadas a grupos mediante la creación de las reglas de directiva correspondientes.

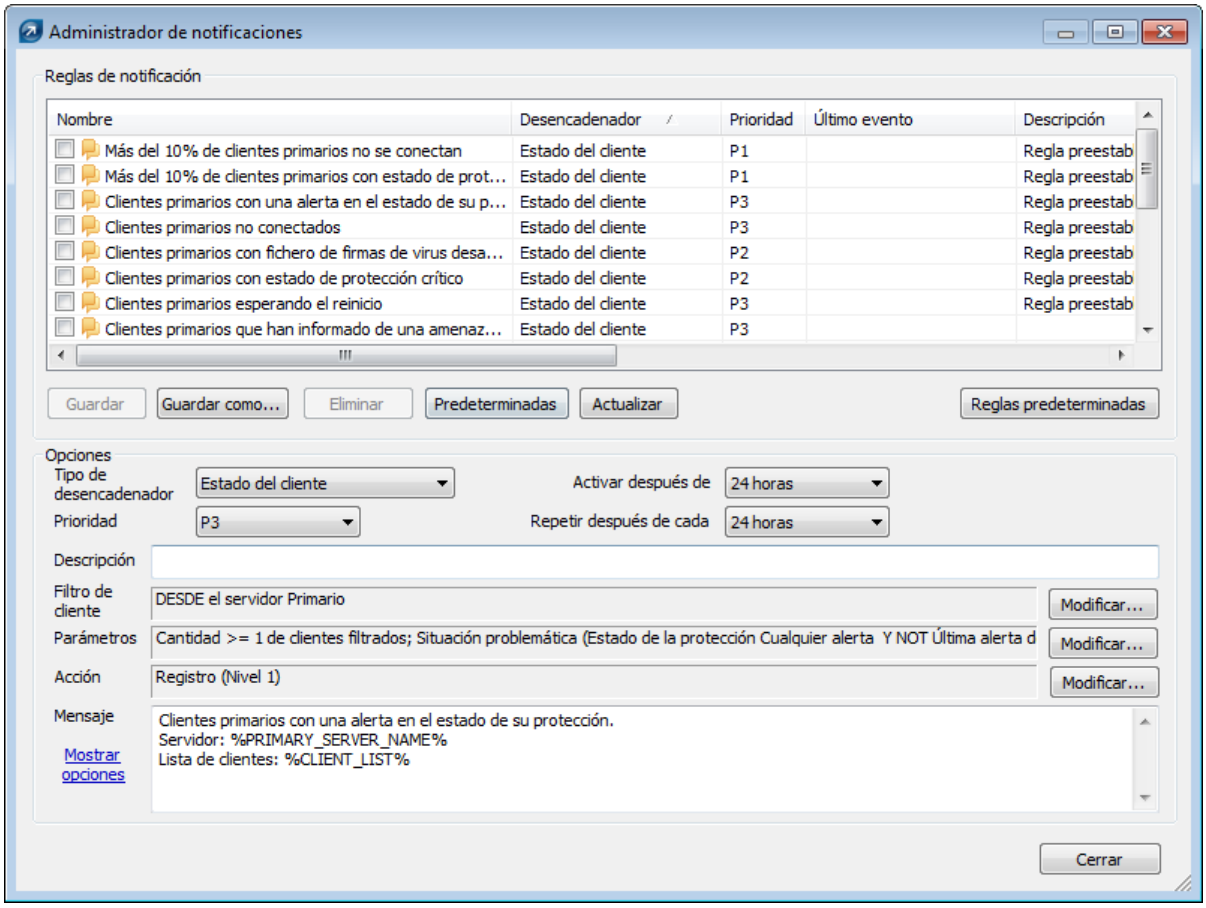
De esta manera, se puede definir una regla de directiva determinada para cada grupo de AD. Ahora, la asignación de una directiva determinada a un cliente determinado depende de la pertenencia del cliente a un grupo de AD. Dado que la sincronización de AD está programada para ejecutarse periódicamente, todos los cambios realizados en la pertenencia del cliente a grupos de AD se actualizan y tienen en cuenta cuando se aplica una regla de directiva. Es decir, las directivas se aplican a los clientes automáticamente en función del grupo de AD al que pertenezcan. Una vez que hayan definido las reglas y directivas de forma exhaustiva, ya no será necesaria la intervención del administrador para la aplicación de directivas.
La principal ventaja de este enfoque es la vinculación directa y automática entre la pertenencia a grupos de AD y la asignación de directivas.

5.4 Notificaciones

La capacidad de notificar a los administradores de la red y del sistema acerca de sucesos importantes es un aspecto esencial de la seguridad e integridad de la red. Una alerta 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 este surgiese más tarde. En los tres apartados siguientes se describen las opciones de notificación que ofrece ERA.

5.4.1 Administrador de notificaciones

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

Entre los botones funcionales de la lista de reglas se encuentran los botones **Guardar** (para guardar modificaciones realizadas en una regla), **Guardar como...** (para guardar notificaciones realizadas en una regla con un nombre nuevo), **Eliminar**, **Predeterminada** (para restaurar la configuración predeterminada del tipo de desencadenador seleccionado), **Actualizar** y **Reglas predeterminadas** (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 del capítulo Creación de reglas 70.

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 algún problema en alguno de los clientes.
- **Estado del servidor**: la regla se ejecutará si hay algún problema en alguno de los servidores.
- **Suceso de tarea finalizada**: la regla se ejecutará cuando 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 definir primero el tipo de desencadenador cuando se creen reglas nuevas.

El menú desplegable **Prioridad** permite definir la prioridad de la regla. **P1** es la prioridad más alta y **P5**, 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 suceso 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 de clientes, 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 principal**: sólo los clientes del servidor principal (se puede usar la forma negativa NO DESDE).
- **Servidor principal EN**: incluye al servidor principal en el resultado.
- **TIENE Indicador Nuevo**: clientes marcados con el indicador *"Nuevo"* (también se puede utilizar la forma negativa NO TIENE).
- **Grupos del administrador remoto EN**: clientes que pertenecen al grupo especificado.
- **Dominio/Grupo de trabajo EN**: clientes que pertenecen al dominio especificado.
- **Máscara de nombre de ordenador**: clientes con el nombre de ordenador indicado.
- **TIENE Máscara IP**: clientes que tengan la máscara IP especificada.
- **TIENE Rango de 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).

Una vez que haya indicado un filtro de clientes para la regla de notificación, haga clic en **Aceptar** para pasar a los parámetros de las reglas. Los parámetros de clientes definen qué condiciones debe cumplir un cliente o un grupo de clientes para que se ejecute la acción de notificación. Para ver los parámetros que 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 por tipo de desencadenador.

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

- **Estado de la protección Cualquier alerta**: cualquier alerta que se encuentre en la columna Estado de la protección.
- **Estado de la protección Alertas graves**: cualquier alerta grave que se encuentre en la columna Estado de la protección.
- **Versión de la base de firmas de virus**: problema con la base de firmas de virus (6 valores posibles).
    - **Anterior**: la base de firmas de virus tiene una versión anterior a la actual.
    - **Anterior o N/D**: la base de firmas de virus tiene una versión más antigua que la anterior o no está disponible.
    - **Anterior a 5 versiones o N/D**: la base de firmas de virus es más de 5 versiones anterior a la actual.
    - **Anterior a 10 versiones o N/D**: la base de firmas de virus es más de 10 versiones anterior a la actual.
    - **Anterior a 7 días o N/D**: la base de firmas de virus es más de 7 días anterior a la actual.
    - **Anterior a 14 días o N/D**: la base de firmas de virus es más de 14 días anterior a la actual.

- **Alerta de última conexión**: la última conexión se estableció antes del período de tiempo especificado.
- **TIENE Último suceso de amenaza**: la columna Amenaza contiene una alerta de amenaza.
- **TIENE Último suceso**: la columna Último suceso contiene una entrada.
- **TIENE Último suceso de cortafuegos**: hay una entrada de suceso del cortafuegos en la columna Suceso de cortafuegos.
- **TIENE Indicador Nuevo**: el cliente tiene el indicador "Nuevo".
- **Esperando para reiniciar**: el cliente está esperando para reiniciarse.
- **Amenaza encontrada del último análisis**: en el cliente, se encontró el número de amenazas especificado durante el último análisis.
- **Amenaza no eliminada en el último análisis**: en el cliente, se encontró el número especificado de amenazas no eliminadas durante el último análisis.

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

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 condiciones**: la regla sólo se ejecuta si se cumplen **todos** los parámetros especificados.
- **se cumplen algunas de las opciones**: la regla 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 superior al especificado.

- **Registros del servidor**: el registro del servidor contiene entradas de estos tipos:

  - **Errores**: mensajes de error.
  - **Errores+Alertas**: mensajes de error y alerta.
  - **Errores+Alertas+Información (nivel de detalle)**: mensajes de error, alerta e informativos.
  - **Filtrar entradas del registro por tipo**: active esta opción para especificar las entradas de error y alerta que 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 lo contrario, las reglas de notificación no detectarán nunca un desencadenador en el registro del servidor. Están disponibles las entradas de registro siguientes:

- **ADSI_SYNCHRONIZE**: sincronización con el grupo de Active Directory.
- **CLEANUP**: tareas de desinfección del servidor.
- **CREATEREPORT**: generación de informes a petición.
- **DEINIT**: apagado del servidor.
- **INIT**: inicio del servidor.
- **INTERNAL 1**: mensaje interno del servidor.
- **INTERNAL 2**: 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 directivas.
- **POLICYRULES**: reglas de directiva.
- **SCHEDREPORT**: informes generados automáticamente.
- **SERVERMGR**: administración de subproceso interno del servidor.
- **SESSION**: conexiones de red del servidor.
- **SESSION_USERACTION**: varias acciones del usuario.
- **THREATSENSE**: ThreatSense.Net, envío de información estadística.
- **UPDATER**: creación de replicaciones 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 ya ha expirado o expirará dentro del número de días indicado. Seleccione la opción **Mostrar alerta 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 expiración 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 desencadenadores de suceso de registro nuevo:
- **Tipo de registro**: seleccione Registro de sucesos, Registro de amenazas o Registro del cortafuegos.
- **Nivel de registro**: nivel de las entradas de registro en el registro en cuestión.
  - Nivel 1 - Alertas graves: sólo errores graves.
  - Nivel 2 - Anteriores + Alerta: igual que el nivel 1, pero con notificaciones de alertas.
  - Nivel 3 - Anteriores + Normal: igual que el nivel 2, pero con notificaciones informativas.

- Nivel 4 - Anteriores + Diagnóstico: igual que el nivel 3, pero con notificaciones de diagnóstico.

- **1000 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 1000 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, la acción definida por el administrador se ejecuta automáticamente. 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; introduzca un **Asunto** y haga clic en **Para** para abrir la libreta de direcciones.
- **Captura de 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. El **Nivel de detalle** de este registro se puede configurar.
- **Registrar también mensaje**: el cuerpo del mensaje también se escribirá en el registro.
- **Registrar en syslog**: registre las notificaciones en registros del sistema; el nivel de detalles de las notificaciones se puede configurar.
- **Registro**: introduce notificaciones en los registros de los servidores; el **Nivel de detalle** de las notificaciones se puede configurar. Para que esta característica funcione correctamente, debe activar el registro en el ERA Server (**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 disponibles, haga clic en **Mostrar opciones**.

- **Server_Last_Updated**: fecha de la última actualización del servidor.
- **Primary_Server_Name**
- **Rule_Name**
- **Rule_Description**
- **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 notificación más reciente (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.
- **Parameters**: 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 expiración.
- **License_Expiration_Date**: fecha de expiración más próxima.
- **License_Clients_Left**: espacios libres en la licencia actual para que más clientes se conecten con el servidor.
- **License_Customer**: cliente con licencia (combinada).
- **Actual_License_Count**: número de clientes conectados actualmente al servidor.
- **Virus_Signature_DB_Version**: versión más reciente de la base de firmas de virus.
- **Pcu_List**: lista de las últimas actualizaciones de componentes del programa.

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** 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** > **Avanzadas** > **Modificar configuración avanzada** > **ESET Remote Administrator** > **Servidor** > **Configuración** > **Notificaciones** > **Intervalo de procesamiento de notificaciones (minutos)**, se puede especificar el intervalo de tiempo durante 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. Tiene a su disposición las siguientes reglas de notificación. Si están activadas y se cumplen las condiciones de las reglas, se 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, la regla se ejecuta lo antes posible.
- **Más del 10% de clientes primarios con estado de protección crítico**: si más del 10 por ciento de los clientes generaron una alerta grave en el estado de protección y no se han conectado durante más de una semana, la regla se ejecuta lo antes posible.
- **Clientes primarios con una alerta en el estado de su protección**: si hay como mínimo un cliente con una alerta 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 firmas de virus 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 alerta 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 ordenador no elimine como mínimo una infección y que no ha estado desconectado durante más de una semana.
- **Tarea finalizadas**: si se finalizó una tarea en un cliente; la regla se ejecuta lo antes posible.
- **Nuevos clientes primarios**: si se ha conectado un cliente nuevo al servidor; la regla se ejecuta lo antes posible.
- **Nuevos clientes replicados**: si hay un cliente replicado nuevo en la lista de clientes; la regla se ejecuta cuando ha transcurrido una hora.
- **Posible brote de virus**: si la frecuencia de las entradas del registro de amenazas supera las 1.000 alertas 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 alertas 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; la 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 la licencia**: si la licencia actual va a expirar en 20 días o menos, después de la expiración, el número máximo de espacios libres para clientes será menor que el número de clientes actual; la 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 extendido 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, el protocolo SNMP se debe instalar y configurar correctamente en el mismo ordenador que el ERAS (**Inicio** > **Panel de control** > **Agregar o quitar programas** > **Agregar o quitar componentes de Windows**). El servicio de SNMP se debe configurar tal como se describe en este artículo: http://support.microsoft.com/kb/315154. En ERAS, debe activar una regla de notificación de SNMP. En ERAS, es necesario activar una regla de notificación de SNMP.

Las notificaciones se pueden ver en el administrador de SNMP, que 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 AdministratorServer\snmp*.

5.4.2 Creación de reglas

En los pasos siguientes se muestra cómo crear una regla que enviará una notificación por correo electrónico al administrador en caso de que haya algún problema con el estado de protección de alguna estación de trabajo cliente. La notificación también se guardará en un archivo llamado *log.txt*.

1) Establezca el menú desplegable **Tipo de desencadenador** en **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 únicamente la condición de la regla de sección **Grupos del administrador remoto EN**. En la parte inferior de esta ventana, haga clic en el vínculo **especificar** y escriba *HQ* en la nueva ventana. Haga clic en **Agregar** y, a continuación, en **Aceptar** (dos veces) para confirmar. Esto indica que la regla sólo se aplicará a clientes del grupo HQ.

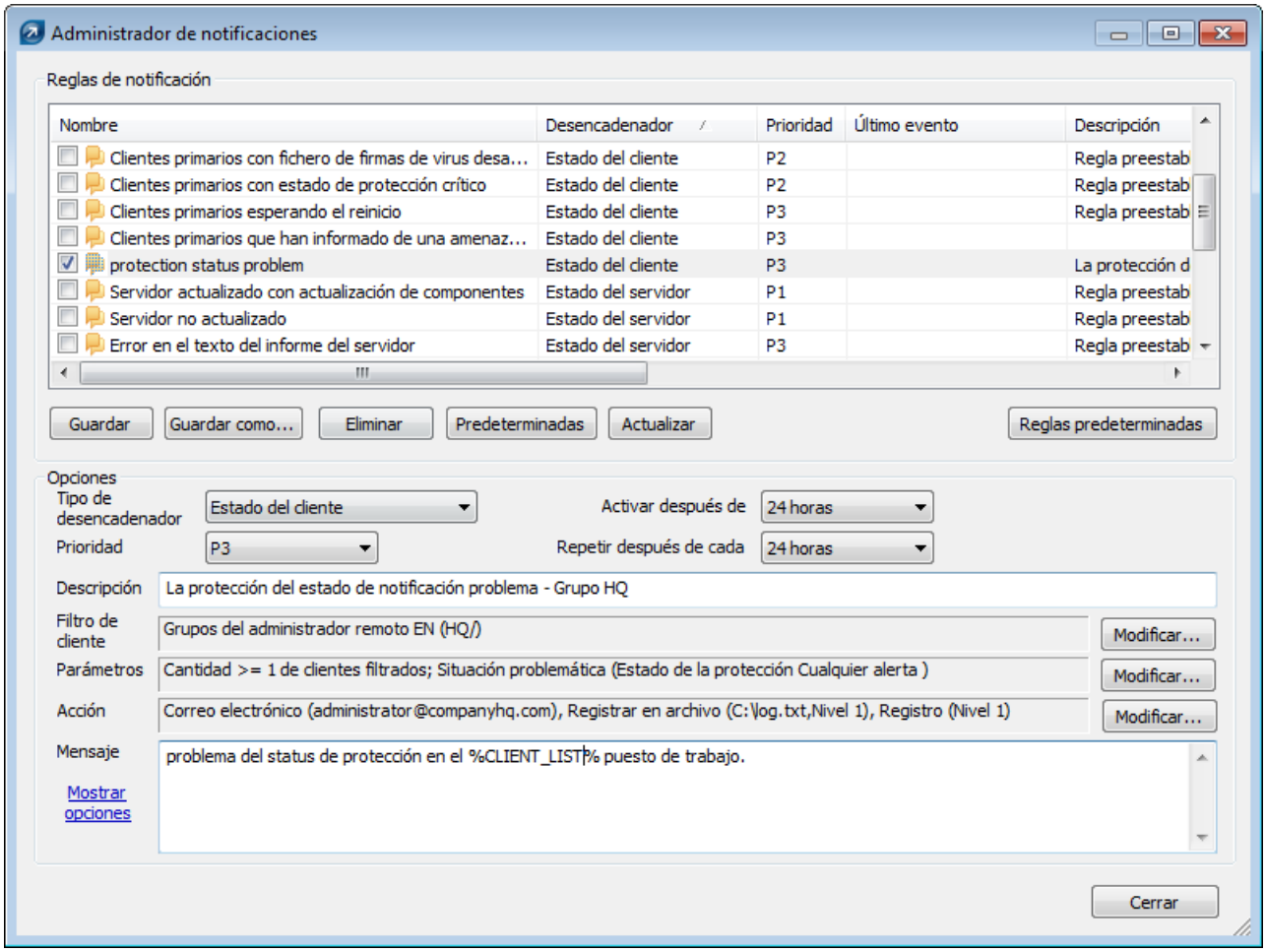
5) Especifique los demás parámetros de la regla en **Parámetros > Modificar...** Anule la selección de todas las opciones, excepto **Estado de la protección Cualquier alerta**.

6) Vaya a la sección **Acción** y haga clic en el botón **Modificar...**. En la ventana **Acción**, active **Correo electrónico**, especifique los destinatarios (**Para...**) y el **Asunto** del mensaje. 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 asignar un nombre a 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 siguiente:



La regla está activa actualmente. Si el estado de protección de un cliente del grupo HQ presenta algún problema, la regla se ejecutará. 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 en ejecución, los programas de inicio, etc. Esta información se puede recuperar con la herramienta integrada ESET SysInspector, que se integra directamente con ERAS. Además de otras funciones de utilidad, ESET SysInspector examina en profundidad el sistema operativo y crea registros del sistema. Para abrirlo, haga clic en **Herramientas** > **ESET SysInspector** en el menú principal de ERAC.

En caso de problemas con un cliente específico, puede solicitar un registro de ESET SysInspector de dicho cliente. Para ello, haga clic con el botón derecho del ratón 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 versiones anteriores no son compatibles con esta característica. Se mostrará una ventana con las opciones siguientes:

- **Crear instantánea (recordar el registro resultante también en el cliente)**: guarda una copia del registro en el ordenador cliente.

- **Incluir comparación con la última instantánea antes de la hora especificada**: muestra un registro comparativo. Los registros comparativos se crean mediante la combinación del registro actual con un registro 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, proceda 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. En la sección superior se muestra un texto informativo sobre los registros más recientes del cliente en cuestión. Haga clic en **Actualizar** para cargar la información más actual.

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 SysInspector 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 ESET SysInspector para ver el archivo abre el registro automáticamente después de guardarlo (igual que tras hacer clic en **Ver**).

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

5.6 Cuarentena centralizada

La cuarentena centralizada es una característica potente que permite a los administradores trabajar fácilmente con archivos en cuarentena de los clientes. Además, facilita operaciones como la visualización, eliminación, restauración y exclusión del análisis de los archivos en cuarentena. Esta característica está disponible en la ventana **Cuarentena** del panel principal de la consola o las propiedades del cliente. En la ventana de cuarentena principal se muestra información completa sobre el archivo, el nombre de la amenaza, el hash, la fecha y hora de la primera y la última repetición, el tamaño del archivo y el número de repeticiones.

NOTA: recuerde que en los campos **Nombre del objeto**, **Nombre de archivo** y **Extensión** se muestran únicamente los tres primeros objetos. Para obtener información detallada, pulse la tecla **F3** o haga doble clic en el elemento seleccionado para abrir la ventana Propiedades.

En Cuarentena centralizada se proporciona información general de los archivos en cuarentena almacenados en los clientes de forma local, con la opción de solicitarlos a petición. Cuando se solicita un archivo, este se copia en el ERA Server de forma segura y cifrada. Por motivos de seguridad, la descodificación se realiza después de guardar el archivo en el disco. Para obtener instrucciones sobre el trabajo con archivos en cuarentena, consulte el capítulo Tarea Restaurar/eliminar de la cuarentena 49.

NOTA: la característica de cuarentena centralizada requiere la instalación de EAV/ESS versión 4.2 (o posterior) en los clientes.

Id. de...	Hash	Fecha de r...	Prime...	Última ocu...	Nombre del o...	Nombre d...	Extensión	Tamaño	Detalle	Recuento ...	Coinciden...	Archivo
3	d27265074...	Hace 64 mi...	Hace 17 ho...	Hace 9 mi...	C:\Users\admi...	eicar_com....	zip	184	Eicar testo...	1	3	No hay dat...
2	bec1b52d3...	Hace 64 mi...	Hace 17 ho...	Hace 9 mi...	C:\Users\admi...	eicarcom2....	zip	308	Eicar testo...	1	3	No hay dat...
1	3395856ce...	Hace 64 mi...	Hace 17 ho...	Hace 11 mi...	C:\Users\admi...	eicar.com[...	txt, com, ...	68	Eicar testo...	1	4	No hay dat...

6. Asistente de combinación de reglas del cortafuegos

El asistente de combinación de reglas del cortafuegos le permite combinar las reglas del cortafuegos de los clientes seleccionados. Esta función es especialmente útil cuando tiene que crear una sola configuración con todas las reglas del cortafuegos recopiladas por clientes en el modo de aprendizaje. Después, la configuración resultante se puede enviar a los clientes mediante una tarea de configuración o se puede aplicar como una directiva.

El asistente está disponible en el menú desplegable **Herramientas** y en el menú contextual de la ficha **Clientes**, al hacer clic con el botón derecho del ratón en los clientes seleccionados (los clientes seleccionados se agregan automáticamente a los elementos seleccionados en el primer paso).

NOTA: para realizar esta acción correctamente, todos los clientes seleccionados deben tener la configuración más reciente almacenada (enviada o replicada) en el servidor.

El proceso es el siguiente: en primer lugar, seleccione los clientes o grupos de clientes con los que se combinarán las reglas del cortafuegos. En el paso siguiente, verá una lista de los clientes seleccionados y su estado de configuración. Si falta la configuración de un cliente en el servidor, puede solicitarla con el botón **Solicitar**. En los últimos pasos, puede seleccionar las reglas combinadas que se utilizarán en la configuración y guardarlas en un archivo *.xml*.

7. Informes

La ficha Informes se utiliza para convertir la información estadística en gráficos o tablas. Estos se pueden guardar y procesar más tarde con el formato de valor separado por comas (*.csv*) utilizando las herramientas de ERA para proporcionar gráficos y otras 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**:

- **Clientes principales con más amenazas**
  Enumera las estaciones de trabajo cliente más "activas" (medido por la cantidad de amenazas detectadas).
- **Usuarios principales con más amenazas**
  Enumera los usuarios más "activos" (medido por la cantidad de amenazas detectadas).
- **Amenazas principales**
  Lista de las amenazas detectadas con mayor frecuencia.
- **Amenazas principales por expansión**
  Muestras las principales amenazas por expansión
- **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 amenaza de los módulos de programa individuales.
- **Amenazas por objeto**
  Número de alertas de amenaza según la ruta por la que intentaron infiltrarse (correos electrónicos, archivos o sectores de inicio).
- **Clientes principales combinados con más amenazas/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.
- **Clientes de grupos**
  Muestra el recuento de clientes de los grupos seleccionados.
- **Clientes de grupos en comparación con todos**
  Muestra la relación porcentual del recuento de clientes de los grupos seleccionados y el recuento total de clientes.
- **Clientes combinados de grupos/Informe de clientes**
  Muestra el recuento de clientes de los grupos seleccionados y los clientes de cada grupo en la tabla (después de hacer clic en el nombre del grupo).
- **Clientes principales con más ataques de red**
  Muestra los clientes principales que presentan más ataques de red.
- **Principales ataques de red**
  Muestra los principales ataques de red.
- **Principales orígenes de los ataques de red**
  Muestra los principales orígenes de los ataques de red.
- **Progreso de los ataques de red**
  Muestra el progreso de los ataques de red.
- **Clientes principales combinados con más ataques de red/Principales ataques de red**
  Muestra los clientes con más ataques de red y los ataques de red principales para cada cliente en la tabla de ataques de red principales (después de hacer clic en el nombre del cliente).
- **Clientes principales con más mensajes SMS no deseados**
  Muestra los clientes principales con más mensajes SMS no deseados.
- **Principales remitentes de mensajes SMS no deseados**
  Muestra los principales remitentes de mensajes SMS no deseados.
- **Progreso de mensajes SMS no deseados**
  Muestra el progreso de mensajes SMS no deseados.

- **Clientes principales combinados con más mensajes SMS no deseados/Principales remitentes de mensajes SMS no deseados**
  Muestra los clientes con más mensajes SMS no deseados y los principales remitentes de mensajes SMS no deseados para cada cliente en la tabla de principales mensajes SMS no deseados (después de hacer clic en el nombre del cliente).
- **Informe de clientes**, **Informe de amenazas**, **Informe del cortafuegos**, **Informe de sucesos**, **Informe de análisis**, **Informe de tareas**, **Informe móvil**, **Informe de cuarentena**
  Informes típicos que se pueden ver en las fichas Clientes, Registro de amenazas, Registro de sucesos, Registro de análisis o Tareas.
- **Informe exhaustivo de amenazas**
  Resumen de Clientes principales combinados con más amenazas/Amenazas principales, Amenazas principales combinadas/Progreso comparativo de amenazas, Progreso de amenazas.
- **Informe exhaustivo de ataques de red**
  Resumen de Clientes principales combinados con más ataques de red/Principales ataques de red, Principales ataques de red, Principales orígenes de los ataques de red, Progreso de los ataques de red.
- **Informe exhaustivo de mensajes SMS no deseados**
  Resumen de Clientes principales combinados con más mensajes SMS no deseados/Principales remitentes de mensajes SMS no deseados, Principales remitentes de mensajes SMS no deseados, Progreso de mensajes SMS no deseados.

En la sección **Filtro** puede utilizar los menús desplegables **Clientes de destino** o **Amenaza** para seleccionar los clientes o virus que 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 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 la 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 (después del sábado).

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

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

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

Una vez que haya programado el informe, haga clic en el botón **Seleccionar objeto...** para especificar dónde se debe guardar el informe. Los informes se pueden guardar en ERAS (de forma predeterminada), enviar por correo electrónico a una dirección concreta o exportar 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 los informes generados por correo electrónico, debe especificar el servidor SMTP y la dirección del remitente en **Herramientas** > **Opciones del servidor** > **Otras opciones**.

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 los 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, independientemente del programa.

Las plantillas de informe existentes se pueden importar o exportar desde/a un archivo *.xml* mediante el botón **Importar.../Exportar...** En la importación, los conflictos de nombre (la plantilla existente y la plantilla importada tienen el mismo nombre) se solucionan agregando una cadena aleatoria al final del nombre de la plantilla importada.

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

Las plantillas de la lista **Favoritos** se pueden usar más tarde para generar informes nuevos de forma inmediata. Para mover una plantilla a Favoritos, haga clic con el botón derecho del ratón en el informe y, a continuación, haga clic en **Agregar a favoritos**, en el menú contextual.

7.1 Situación de creación de informe de ejemplo

Para mantener la seguridad de la red de los clientes al máximo nivel, deberá estar bien informado del estado de seguridad de la red. Puede crear informes con toda la información sobre amenazas, actualizaciones, versiones de producto del cliente, etc. de forma sencilla (consulte el apartado Informes 74 para obtener más información). Normalmente, bastará con un informe semanal para proporcionar toda la información necesaria. Sin embargo, es posible que en algunos caso sea necesaria más vigilancia, como cuando se detecta una amenaza.

A modo de ejemplo, crearemos un grupo paramétrico llamado *Cuarentena*. Este grupo incluirá únicamente a ordenadores en los que se haya detectado y eliminado una amenaza durante el último análisis a petición realizado. Para establecer esta condición, seleccione la opción **TIENE Amenaza encontrada del último análisis**. Para crear este grupo paramétrico, siga las instrucciones del apartado Grupos paramétricos 52.

NOTA: cuando cree el grupo *Cuarentena*, asegúrese de que la opción **Permanente** no está activada. El ordenador se asignará de forma dinámica y se eliminará cuando no se cumplan las condiciones.

Cree el informe *Ordenadores en cuarentena*. Para crear este grupo paramétrico, siga las instrucciones del apartado Informes 74.
A continuación se indica la configuración específica de nuestro ejemplo:

- Ajustes comodín de **Opciones**:

Tipo: **Informe de cuarentena con detalles**
Estilo: **Tema azul**
Clientes de destino: **Sólo los grupos seleccionados**
Amenaza: **N/D**

- Ajustes comodín de **Intervalo**:

Actual: **Día**

- Ajustes comodín de **Programador de Tareas**:

Frecuencia: **Diariamente**
Cada: **1 día**

SUGERENCIA: puede almacenar los resultados en la base de datos de informes o definir una carpeta para guardar copias de los informes. Los informes también se pueden enviar por correo electrónico. Estos ajustes están disponibles al hacer clic en el botón **Seleccionar objeto...**

Los informes generados se pueden revisar en el comodín **Informes generales** de la sección **Informes**.

Resumen: creamos el grupo paramétrico *Cuarentena*, que contiene ordenadores para los que se informó de una amenaza durante el análisis a petición más reciente. Después, creamos un informe automático que nos informará, diariamente, de los ordenadores que pertenecen al grupo *Cuarentena* y nos proporcionará información general sobre el estado de la red de nuestro cliente, lo que nos permitirá controlar las posibles amenazas.

SUGERENCIA: si desea ver los detalles del registro de análisis más reciente, utilice el tipo de informe **Informe de análisis detallado**.

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

8.1 Seguridad

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

Las anteriores versiones (2.x) no cuentan con esta función. Para permitir la compatibilidad con las versiones anteriores, active el modo **Activar acceso sin autenticación para clientes**.

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

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

- **Contraseña para la replicación**
  Establece una contraseña para los ERA Server inferiores si se replican en un servidor ERAS determinado.

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

- **Activar acceso no autenticado para clientes (productos de seguridad de ESET)**
  Permite el acceso a 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 autenticación para replicación**
  Permite el acceso a ERAS a los clientes del ERA Server inferiores que no cuentan con una contraseña válida para la replicación especificada.

- **Activar acceso no autenticado para el instalador remoto de ESET (Agente)**
  Activa el acceso a ERAS para el instalador remoto de ESET, que no tiene una contraseña válida especificada.

NOTA: si se activa la autenticación en ERAS y en todos los clientes (generación 3.x y posterior), se puede desactivar la opción **Activar acceso sin autenticación para clientes**.

- **Utilizar autenticación de dominio de Windows**
  Activa la autenticación del dominio de Windows y le permite definir grupos de administrador (con acceso completo al ERA Server) así como grupos con acceso de sólo lectura (se activa con la opción **Conceder a los demás usuarios acceso de sólo lectura**).

8.2 Mantenimiento del servidor

Si se configura correctamente en la ficha Mantenimiento del servidor, la base de datos de ERAS se mantendrá y optimizará automáticamente, sin necesidad de realizar ninguna configuración adicional. 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**.

Estas opciones son, entre otras:

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

- **Eliminar registros móviles anteriores a X meses (días)**
  Elimina todos los registros móviles anteriores al número de meses (o días) especificado.

- **Eliminar entradas en cuarentena sin clientes anteriores a X meses (días)**
  Elimina todos los registros de análisis anteriores al número de meses (o días) especificado.

Programador de desinfección
Ejecuta la opción seleccionada más arriba cada ... minutos.

Programador para Compactar y reparar
Compacta la base de datos con un intervalo de tiempo específico y a una hora determinada. La operación de compactar y reparar elimina inconsistencias y problemas, y hace que la comunicación con la base de datos sea más rápida.

8.3 Servidor Mirror

La característica Mirror permite al usuario crear un servidor de actualización local. Los ordenadores cliente no descargarán actualizaciones de firmas de virus de los servidores de ESET en Internet, sino que se conectarán a un servidor Mirror local de 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 para las actualizaciones únicamente se conecta a Internet el servidor Mirror, en lugar de que lo hagan cientos de máquinas cliente. Esta configuración significa que es importante que el servidor Mirror esté siempre conectado a Internet.

Alerta: un servidor Mirror 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 distribuirla 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 a los Mirrors creados en ERAS.

La característica Mirror está disponible en dos ubicaciones:

- ESET Remote Administrator (el Mirror que se ejecuta físicamente en ERAS, y se puede administrar desde ERAC)

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

El administrador selecciona el método de activación de la característica Mirror.

En grandes redes, es posible crear varios servidores Mirror (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 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 característica Mirror en 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, el nombre de usuario y la contraseña para actualizaciones superiores de ESET Smart Security Business Edition.

NOTA: los clientes de ESET NOD32 Antivirus también se pueden actualizar con una licencia de ESET Smart Security, pero no al revés.

8.3.1 Funcionamiento del servidor Mirror

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

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

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

El servidor Mirror, 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 autenticación), compruebe que no sea accesible desde fuera de su red (es decir, por clientes que no estén incluidos en su licencia). El servidor no debe ser accesible desde Internet.

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

NOTA: si se está utilizando el método del servidor HTTP, se recomienda utilizar un máximo de 400 clientes para la actualización desde un Mirror. En las redes grandes que tienen más clientes, es recomendable repartir las actualizaciones del Mirror entre varios servidores Mirror de ERA (o ESS/EAV). Si es necesario centralizar el Mirror en un solo servidor, es recomendable utilizar otro tipo de servidor HTTP, como Apache. ERA también es compatible con métodos de autenticación adicionales (en Apache Web Server, por ejemplo, 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 introducir en la estación de trabajo cliente un nombre de usuario y una contraseña de usuario con permisos de "lectura" para la carpeta de actualización.

NOTA: las soluciones cliente de ESET utilizan la cuenta de usuario SYSTEM y, por lo tanto, tienen permisos de acceso a la red diferentes a los de un usuario registrado. La autenticación es necesaria aunque la unidad de red sea accesible para "Todos" y el usuario actual también disponga de 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 ordenadores cliente exclusivamente para 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 autenticación en una unidad de red, indique los datos de autenticación de forma completa: *GRUPODETRABAJO\Usuario* o *DOMINIO\Usuario*.

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

8.3.2 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 están disponibles actualizaciones de componentes del programa. Las actualizaciones de componentes del programa añaden nuevas características a los productos de seguridad de ESET y requieren el reinicio.

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

Esta característica es especialmente útil si el administrador desea descargar y usar actualizaciones de base de firmas de virus cuando sólo está disponible una nueva versión del programa. Si se usa una versión anterior del programa junto con la versión más reciente de la 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 características del programa.

De forma predeterminada, los componentes del programa no se descargan automáticamente y deben configurarse manualmente en ERAS. Para obtener más información, consulte el apartado Cómo activar y configurar el Mirror 80.

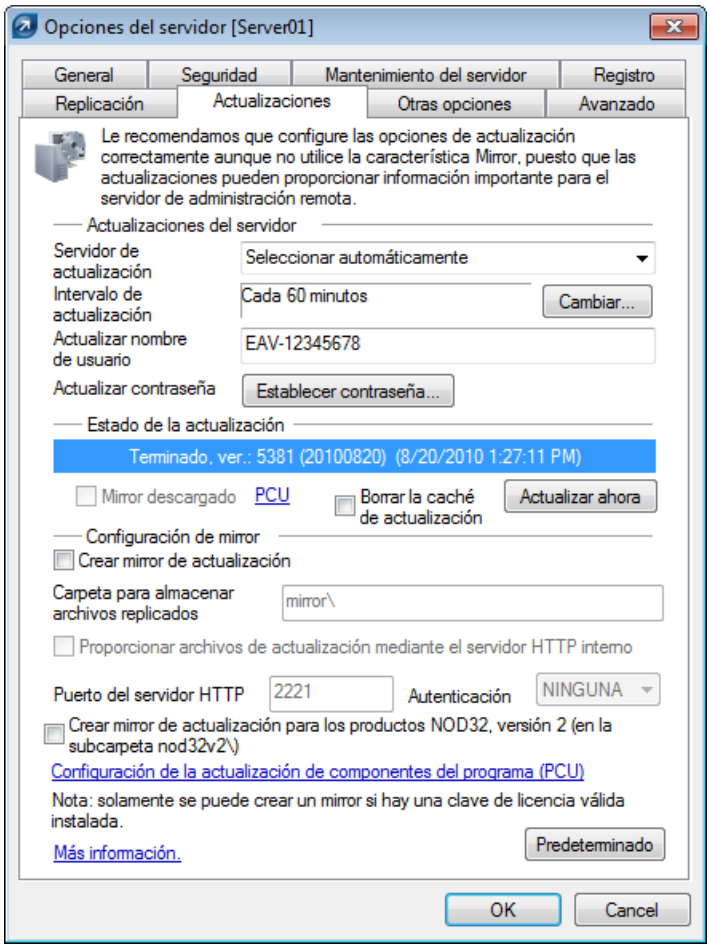
8.3.3 Cómo activar y configurar el Mirror

Si el Mirror está directamente integrado en ERA (un componente de Business Edition), conéctese a ERAS mediante ERAC y siga estos pasos:

- Desde ERAC, haga clic en **Herramientas** > **Opciones del servidor...** y, a continuación, en **Actualizaciones**.
- En el menú desplegable del **Servidor de actualización**, elija **Seleccionar automáticamente** (las actualizaciones se descargarán de los servidores de ESET) o especifique la ruta de acceso de *URL/UNC* a un servidor Mirror.
- 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 la contraseña (Actualizar contraseña) que se enviaron después de la compra. Si accede a un servidor superior, indique un nombre de usuario y una contraseña de dominio válido para dicho servidor.
- Seleccione la opción **Crear mirror 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 Mirror, siempre que la opción **Proporcionar archivos de actualización mediante el servidor HTTP interno** esté seleccionada y disponible en el puerto HTTP definido en el campo **Puerto de servidor HTTP** (2221, de forma predeterminada). Establezca la **Autenticación** en **NINGUNA** (consulte el capítulo Funcionamiento del servidor Mirror 79 para obtener más información).

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

- La opción **PCU descargadas del mirror** le permite activar la replicación de componentes del programa. Para configurar la replicación de componentes de actualización del programa, acceda a **Avanzadas > Modificar configuración avanzada** y configure los ajustes de **ESET Remote Administrator** > **ERA Server** > **Configuración > Mirror** (o **Mirror para NOD32 versión 2**).
- Seleccione los componentes de idioma que desea descargar en **Avanzadas** > **Modificar configuración avanzada...**, sección **ERA Server** > **Configuración** > **Mirror** > **Crear mirror 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 la descarga de una versión de idioma que no está instalada en la red aumentará el tráfico de red de forma innecesaria.



La característica Mirror también está disponible directamente en la interfaz del programa de ESET Smart Security Business Edition y ESET NOD32 Antivirus Business Edition. Se deja a discreción del administrador la decisión de dónde implementar el servidor Mirror.

Para activar e iniciar el servidor Mirror desde 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**. La licencia se instalará y le permitirá configurar la característica Mirror.

3) En la sección **Actualizar**, haga clic en el botón **Configuración...** y seleccione la ficha **Mirror**.

4) Seleccione las opciones **Crear mirror 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 replicados**) en la que se guardarán los archivos de actualización.

6) El **nombre de usuario** y la **contraseña** sirven como datos de autenticación para las estaciones de trabajo cliente que intentan obtener acceso a la carpeta de mirror. En la mayoría de los casos, no es necesario rellenar estos campos.

7) Establezca la autenticación en **NINGUNA**.

8) Seleccione los componentes que desea descargar (seleccione los componentes para todas las versiones de idioma que se usarán en la red). Los componentes sólo se muestran si están disponibles en los servidores de actualización de ESET.

NOTA: para mantener una funcionalidad óptima, recomendamos que active la descarga y la replicación de los componentes del programa. Si esta opción está desactivada, sólo se actualiza la base de firmas de virus, no los componentes del programa. Si se utiliza el Mirror como parte de ERA, esta opción se puede configurar en ERAC a través de la ficha **Herramientas** > **Opciones del servidor...** > **Avanzadas** > **Modificar configuración avanzada...** > **ESET Remote Administrator** > **ERA Server** > **Configuración** > **Mirror**. Active todas las versiones de idiomas del programa

que estén disponibles en su red.

8.3.4 Mirror para clientes con NOD32 versión 2.x

ESET Remote Administrator también permite al administrador crear copias del archivo de actualización para los ordenadores cliente que tengan instalado ESET NOD32 Antivirus 2.x. Para ello, haga clic en **Herramientas** > **Opciones del servidor** > **Actualizaciones** > **Crear mirror de actualización para los productos NOD32, versión 2**. Esto sólo se aplica a ERA. El Mirror de la solución cliente de Business Edition (v 3.x) no incluye esta opción.

Si dispone de una mezcla de clientes 2.x y 3.x en su red, se recomienda utilizar el Mirror integrado en ERA. Si ambos Mirrors están activados en el mismo ordenador, uno en ERAS para clientes 2.x y otro en un cliente Business Edition para clientes 3.x, se podría provocar un conflicto entre dos servidores HTTP que utilicen el mismo puerto TCP.

Las actualizaciones para clientes 2.x se guardan en la carpeta *"nod32v2"*, una subcarpeta de la carpeta de mirror principal. Está disponible en la dirección URL:

http://Nombre_del_servidor_Mirror :puerto/nod32v2

o ruta de acceso UNC a una unidad de red:

\\Nombre_del_servidor_Mirror/nombre_de_uso_compartido\nod32v2

ERA también puede descargar componentes de programa para clientes 2.x. Para seleccionar los componentes del programa que desea descargar, vaya a la ficha **Herramientas** > **Opciones del servidor...** > **Avanzadas**, haga clic en **Modificar configuración avanzada...** y expanda la sección **ESET Remote Administrator** > **ERA Server** > **Configuración** > **Mirror para NOD32 versión 2**. Para minimizar el volumen de datos descargados, seleccione sólo las versiones de idioma que estén disponibles en su red.

8.4 Replicación

La replicación se utiliza en redes de gran tamaño, donde hay instalados varios ERA Server (p. ej., una empresa con varias sucursales). Para obtener más información, consulte el capítulo Instalación 17.

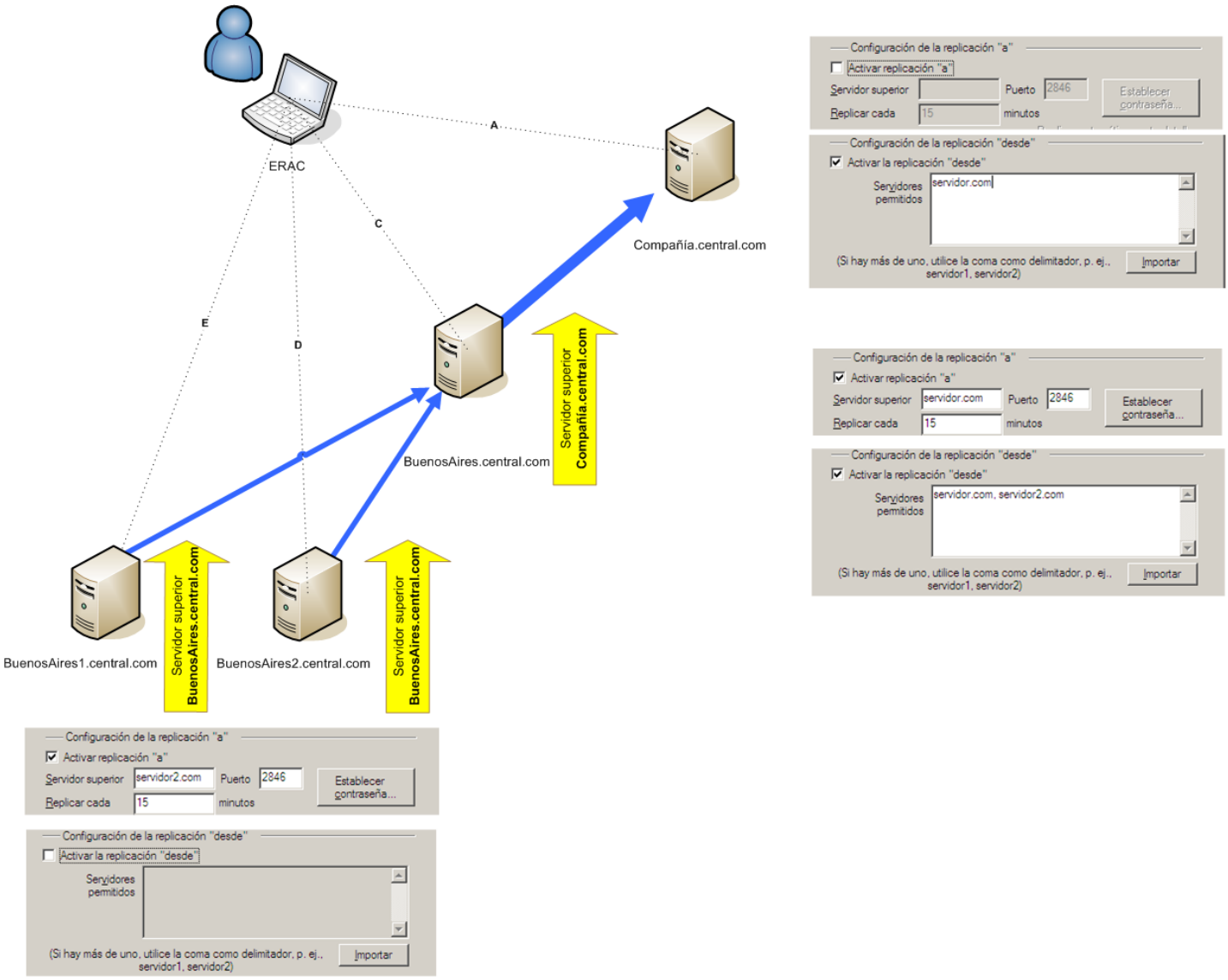
Las opciones de la ficha Replicación (**Herramientas > Opciones del servidor...**) se dividen en dos secciones:

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

La sección **Configuración de la replicación "a"** se usa para configurar ERA Server inferiores. Se debe activar la opción **Activar replicación "a"** y especificar la dirección IP o el nombre de ERAS maestro (servidor superior). Por tanto, los datos del servidor inferior se replican al servidor maestro. La opción **Configuración de la replicación "desde"** permite a los ERA Server maestro (superiores) aceptar datos de ERA Server inferiores, así como transferirlos a sus servidores maestro. 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 los ERA Server ubicados en la mitad de la jerarquía de replicación (es decir, que tengan tanto servidores inferiores como superiores).

Todas las situaciones anteriores se pueden ver en la imagen que se muestra a continuación. Los ordenadores de color beis representan ERA Server individuales. Cada ERAS se representa con su nombre (que debe ser el mismo que *% Computer Name%* para evitar confusiones) y con la configuración correspondiente en la ventana de diálogo de la replicación.



Las demás 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**, **Replicar registro móvil**, **Replicar registro de cuarentena**
  Si se seleccionan estas opciones, toda la información mostrada en la ficha **Clientes**, **Registro de amenazas**, **Registro del cortafuegos**, **Registro de sucesos**, **Registro de análisis**, **Registro móvil**, **Registro de cuarentena** y **Tareas** se replican en columnas y líneas 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 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**, **Replicar automáticamente detalles del registro móvil**, **Replicar automáticamente archivos en cuarentena**
  Estas opciones activan la replicación automática de la información complementaria almacenada en archivos individuales. También se pueden descargar 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 se debe 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 una gran cantidad de espacio en el disco. Normalmente, dicha información no es necesaria y se puede solicitar manualmente. Los servidores secundarios no envían información sobre clientes eliminados de forma automática. Por tanto, los servidores superiores pueden continuar almacenando información sobre clientes eliminados procedente de los servidores inferiores. Si desea eliminar un cliente de la ficha Cliente en servidores superiores, seleccione la opción Activar la eliminación de clientes replicados en el servidor subyacente, disponible en **Opciones del servidor** > **Avanzadas** > **Modificar configuración avanzada** > **Configurar** > **Replicación**.

Para establecer el nivel de mantenimiento del registro en ERAS, haga clic en **Herramientas** > **Opciones del servidor** >

Avanzadas > **Modificar configuración avanzada...** > **Configuración** > **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"**.

8.5 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 sucesos del sistema (**Panel de control de Windows** > **Herramientas administrativas** > **Visor de sucesos**).

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 si así se lo aconseja el servicio de atención al cliente de ESET.

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

8.6 Administración de licencias

Para que ERA funcione correctamente, debe cargar una clave de licencia. Después de la adquisición, las claves de licencia se le enviarán, junto con el nombre de usuario y la contraseña, a su dirección de correo electrónico. El **Administrador de licencias** sirve para administrar 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.

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

Para agregar una clave de licencia nueva:

1) Vaya a **Herramientas** > **Administrador de licencias** o pulse **CTRL+L** en el teclado.
2) Haga clic en **Examinar** y busque el archivo de clave 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 una clave de licencia (mediante el botón **Examinar**). La información acerca de la clave de licencia visualizada actualmente se muestra en esta 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 la clave de licencia que se 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, ERAS tratará siempre de encontrar la clave que tenga más clientes y con la fecha de expiración 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 expiración de la nueva clave de licencia es igual a la fecha de la clave que antes expire.

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 expirar en 20 días**: muestra una alerta x días antes de que la licencia expire.
- **Mostrar alerta 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 alerta sólo si la expiración 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 de ERAS.
- **Advertir si sólo queda un 10% de clientes libres en las licencias del servidor**: el servidor mostrará una alerta si el número de espacios libres para clientes cae por debajo de un valor indicado (expresado como porcentaje).

ERAS es capaz de combinar varias licencias procedentes de varios clientes. Esta característica 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.

8.7 Configuración avanzada

Para acceder a la configuración avanzada de ERA, haga clic en **Herramientas** > **Opciones del servidor** > **Avanzadas** > **Modificar configuración avanzada**.

La configuración avanzada incluye lo siguiente:

- **Uso máx. de espacio en disco (porcentaje)**
  En caso de que se supere, es posible que algunas características del servidor no estén disponibles. Cuando se conecta a ERAS, 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 direcciones MAC (como ESET NOD32 Antivirus 2.x) a una solución cliente que sí lo es (como un cliente 3.x), el antiguo registro cliente se convierte al 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 es compatible con el envío de direcciones MAC (como ESET NOD32 Antivirus 3.x) a una solución cliente que no lo es (como un cliente 2.x), el antiguo registro cliente se convierte al 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 se identifica como el mismo cliente tras cambiar la dirección MAC.
- **Activar cambio de nombre del ordenador**
  Permite el cambio de nombre de los ordenadores cliente. Si esta opción está desactivada, el nombre del ordenador formará parte de la identificación única de los clientes.
- **Utilizar también el registro del servidor predeterminado durante la instalación impulsada**
  ERAS permite al usuario definir el nombre de usuario y la contraseña sólo para la instalación remota por scripts de inicio de sesión y correo electrónico. Active esta opción para usar los valores predefinidos también para las instalaciones remotas impulsadas.

8.8 Otras opciones

Configuración SMTP
Algunas características de ERA requieren una correcta configuración del servidor SMTP. Estas características incluyen la instalación remota por correo electrónico y la generación de informes para su envío por correo electrónico.

Nuevos clientes

Permitir nuevos clientes
Si está desactivado, no se añadirán clientes nuevos en la ficha Clientes (aunque se comuniquen con ERA Server, los clientes nuevos no serán visibles en la ficha Clientes).

Restablecer automáticamente el indicador "Nuevo" según los nuevos clientes
Si está activada, el indicador "Nuevo" se elimina de los clientes que se conectan a ERAS por primera vez. Para obtener

más información, consulte el capítulo Ficha Clientes 25.

Puertos
Le permite personalizar los puertos donde ERAS está a la escucha de comunicaciones; los puertos se establecen por **Consola** (de forma predeterminada, 2223), **Cliente** (de forma predeterminada, 2222), proceso de replicación (**Puerto de replicación** (de forma predeterminada, 2846), **Instalador remoto de ESET** (de forma predeterminada, 2224).

ThreatSense.Net
Si está activada, ERAS enviará los archivos sospechosos y la información estadística de los clientes a los servidores de ESET con los intervalos de tiempo especificados. Tenga en cuenta que las estaciones de trabajo cliente no siempre pueden enviar esta información directamente, debido a la configuración de la red.

9. ESET Remote Administrator Maintenance Tool

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

NOTA: Para que ERA Maintenance Tool funcione correctamente en Windows NT4 SP6, se requiere Internet Explorer v5.O o posterior o, al menos, actualizar la biblioteca de controles comunes (comctl32.dll). La biblioteca ComCtl32 forma parte de los redistribuibles Comctl32 de Platform SDK y está disponible para su descarga en el Sitio web de Microsoft.

9.1 Información del ERA Server

La herramienta muestra información resumida sobre el ERA Server instalado. La información que se muestra se puede ver con más detalle, en una ventana independiente, haciendo clic en **Más información**, se puede copiar con la opción **Copiar al Portapapeles** y se puede actualizar con la opción **Actualizar**. Una vez comprobada la información, haga clic en **Siguiente** para ir al paso siguiente.

9.2 Tipo de tarea

La herramienta de mantenimiento contiene la lista de las tareas disponibles. Después de configurar una tarea, haga clic en **Guardar todos los parámetros en un archivo** para guardar sus ajustes. Los ajustes se pueden usar en cualquier momento haciendo clic en **Cargar todos los parámetros de un archivo**. Cada paso individual de 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**.

9.2.1 Detener el ERA Server

Esta tarea detiene el servicio de ESET Remote Administrator Server.

9.2.2 Iniciar el ERA Server

Esta tarea inicia el servicio del Server de ESET Remote Administrator.

9.2.3 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 consiste en seleccionar la base de datos.

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

- Cadena de conexión: cadena especial que se usa para identificar la base de datos de origen.
- Nombre de usuario: nombre de usuario que se usa para acceder a la base de datos.
- Contraseña: contraseña que se usa 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 ajustes actuales de ERA Server. 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 corrección de la base de datos, haga clic en **Siguiente**.

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

Especifique, para todos los tipos de base de datos (además de la base de datos de MS Access), si desea crear las tablas

de base de datos automáticamente (**Crear tablas en la base de datos automáticamente**) o insertarlas en la base de datos más adelante (**Ver script** > **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 base de datos MYSQL nueva con el nombre ESETRADB. En el último paso, se confirma la conversión de la base de datos.

9.2.4 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 ajustes de la primera ventana son similares a los de la conversión de la base de datos (consulte el capítulo Transferencia de la base de datos 87). Aquí se selecciona la base de datos de origen. Después, la base de datos de origen se copiará en un archivo de copia de seguridad, que se especificará en el paso siguiente.

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

9.2.5 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 ajustes de la primera ventana son similares a los de la conversión de la base de datos (consulte el capítulo Transferencia de la base de datos 87). Aquí se selecciona el tipo de base de datos.

Especifique, para todos los tipos de base de datos (además de la base de datos de MS Access), si desea crear las tablas de base de datos automáticamente (**Crear tablas en la base de datos automáticamente**) o insertarlas en la base de datos más adelante (**Ver script** > **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 base de datos MYSQL nueva con el nombre ESETRADB. En el último paso, se confirma la conversión de la base de datos.

Seleccione el archivo desde el que se restaurará la base de datos en el paso siguiente. Los parámetros opcionales situados en la parte inferior de la ventana le permiten importar un archivo desde un tipo de base de datos distinto al seleccionado en el paso anterior (**Permitir importar desde un tipo de base de datos diferente**), así como detener ESET Remote Administrator Server 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.

9.2.6 Eliminar tablas

Esta opción elimina las tablas que haya en la base de datos en ese momento. Como resultado, la base de datos volverá al estado en que se encontraba justo después de la instalación del ERA Server. Los ajustes de la primera ventana son similares a los de la conversión de la base de datos (consulte el capítulo Transferencia de la base de datos 87). Aquí se selecciona el tipo de base de datos. En el paso siguiente se le solicitará que confirme la acción. Seleccione **Sí, acepto** y, a continuación, haga clic en **Siguiente** para confirmar la acción.

NOTA: si se utiliza una base de datos MS SQL, My SQL o Oracle, es recomendable detener el ERA Server antes de eliminar las tablas.
Si se utiliza una base de datos de MS Access, esta se sustituirá por la base de datos vacía predeterminada.

9.2.7 Instalación de una clave de licencia nueva

Para insertar una clave de licencia nueva para usarla con el servidor, escriba su ubicación.
Si es necesario, sobrescriba la clave de licencia existente (**Sobrescribir si existe**) y reinicie el servidor (**Forzar el inicio del servidor (si no se está ejecutando)**). Haga clic en **Siguiente** para confirmar y efectuar la acción.

9.2.8 Modificación de la configuración del servidor

Esta tarea inicia Configuration Editor (si está instalado). Al finalizar la tarea se abre la ventana de Configuration Editor, donde podrá modificar la configuración avanzada del ERA Server. Estos ajustes están disponibles en **Herramientas** > **Opciones del servidor** > **Avanzadas** > **Modificar configuración avanzada**.

NOTA: para que esta característica funcione, la ERA Console debe estar instalada.

10. Resolución de problemas

10.1 Preguntas frecuentes

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

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

Causa:
Una de las posibles causas puede ser que Terminal Server está activado en el sistema en el modo de *ejecución*.

Solución:
Microsoft aconseja activar el modo de *instalación* de Terminal Server durante la instalación de programas en un sistema que tenga el servicio de Terminal Server activo. Esto se puede hacer a través de **Panel de control** > **Agregar o quitar programas**, o abriendo una ventana de símbolo del sistema para emitir el comando *change user /install*. Tras la instalación, escriba *change user/execute* para devolver Terminal Server al modo de ejecución. Para obtener las instrucciones detalladas de este proceso, consulte el siguiente artículo: http://support.microsoft.com/kb/320185.

10.1.2 ¿Qué significa el código de error GLE?

La instalación de ESET Smart Security o ESET NOD32 Antivirus mediante ESET Remote Administrator Console podría generar un error GLE. Para descubrir el significado de un número de error GLE, siga estos pasos:

1) Haga clic en **Inicio** > **Ejecutar** para abrir una ventana de símbolo del sistema. Escriba *cmd* y haga clic en **Aceptar**.
2) En la ventana de símbolo del sistema, escriba: *net helpmsg número_error*

Ejemplo: *net helpmsg 55*

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

10.2 Códigos de error que aparecen con frecuencia

Durante el funcionamiento de ERA, puede encontrarse mensajes de error con códigos de error que indican la existencia de un problema en alguna característica u operación. En los capítulos siguientes se describen los códigos de error más frecuentes al realizar instalaciones impulsadas, así como los errores que se pueden encontrar en el registro de ERAS.

10.2.1 Mensajes de error generados al utilizar ESET Remote Administrator para instalar ESET Smart Security o ESET NOD32 Antivirus de forma remota

Código de error SC 6, código de error GLE 53. No se ha podido configurar la conexión IPC con el ordenador de destino
Para configurar una conexión IPC, deben cumplirse estos requisitos:
1. Conjunto de TCP/IP instalado en el mismo ordenador que ERAS, así como en el ordenador de destino.
2. Debe instalarse el uso compartido de archivos e impresoras para Microsoft Network.
3. Los puertos de uso compartido de archivos (135-139, 445) deben estar abiertos.
4. El ordenador 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 ordenador de destino
El recurso compartido administrativo *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 ordenador 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 ordenador de destino
El campo de contraseña del administrador está vacío. La 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 ordenador de destino
El instalador no puede acceder al ordenador cliente porque no tiene privilegios de acceso suficientes (Acceso denegado).

Código de error SC 11, código de error GLE 1726. No se ha podido instalar el instalador de NOD32 en el ordenador 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.

10.2.2 Códigos de error que aparecen con frecuencia en el registro era.log

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, salvo los valores 401, 403, 404 y 407.
  - Si las actualizaciones se descargan desde un servidor CISCO y el formato de respuesta de autenticación de HTML ha cambiado.

- Al actualizar desde una carpeta compartida:
  - El error devuelto no entra en las categorías "mala autenticación" o "archivo no encontrado" (por ejemplo, *conexión interrumpida* o *servidor no existente*).

- Ambos métodos de autenticación:
  - Si no se encuentra ninguno de los servidores del archivo *upd.ver* (el archivo se encuentra 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 ERAS:
  - El administrador debe especificar el servidor proxy en el formato.

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

0x2102 - UPD_RETVAL_BAD_REPLY
Este error de módulo de actualización se puede encontrar si se utiliza un servidor proxy para mediar en una conexión a Internet, en concreto un proxy Webwasher.

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

0x2105 - UPD_RETVAL_INTERRUPTED
Este error del módulo de actualización se puede encontrar si se utiliza un servidor proxy para mediar en una conexión a Internet, en concreto un proxy Webwasher.

10.3 ¿Cómo diagnosticar problemas con ERAS?

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

1) Revise el registro de ERAS: haga clic en **Herramientas** > **Opciones del servidor** en el menú principal de ERAC. En la ventana **Opciones del servidor**, haga clic en la ficha **Registro** y, a continuación, en **Ver registro**.

2) Si no ve mensajes de error, suba el nivel de **Contenido del registro**, en la ventana **Opciones del servidor**, hasta el Nivel 5. Una vez que haya localizado el problema, recomendamos que restablezca el valor predeterminado.

3) También puede solucionar problemas activando el registro de depuración de la base de datos en la misma ficha. Consulte la sección **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, ERAS, ERAC, ESET Smart Security, ESET NOD32 Antivirus).

11. Ayudas y sugerencias

11.1 Programador de Tareas

ESET NOD32 Antivirus y ESET Smart Security contienen un programador de tareas integrado que permite la programación periódica de análisis, actualizaciones, etc. Todas las tareas especificadas se muestran en el Programador de Tareas.

ERA permite configurar los siguientes tipos de tareas:

- Ejecutar aplicación externa
- Mantenimiento de registros
- Análisis del ordenador
- Crear una instantánea de estado del ordenador
- Actualizar
- Análisis automático de archivos durante el inicio del sistema

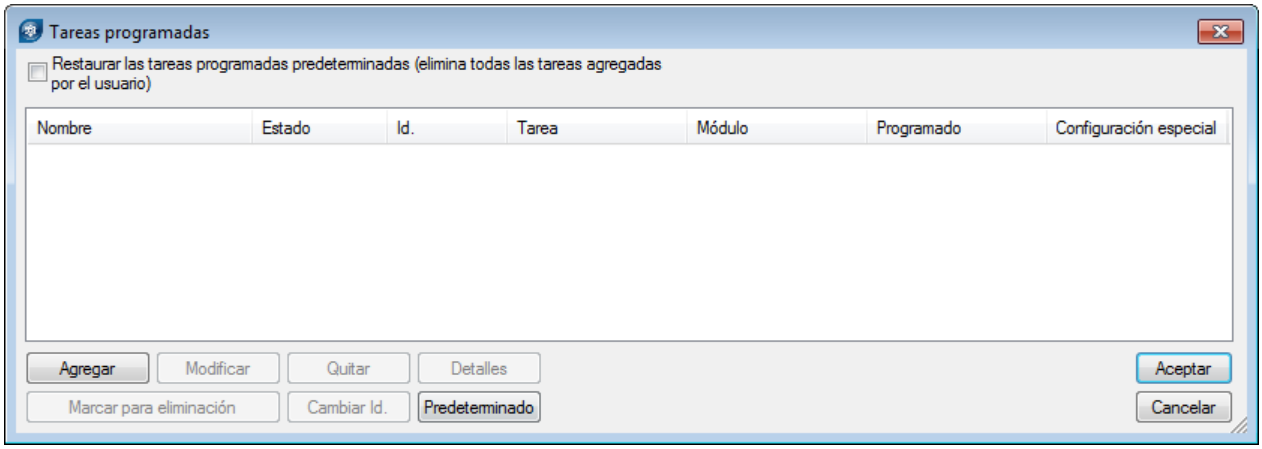
En la mayoría de los casos, no es necesario configurar una tarea **Ejecutar aplicación externa**. La tarea **Análisis automático de archivos durante el inicio del sistema** es una tarea predeterminada y no es recomendable modificar sus parámetros. Si no se han realizado cambios tras la instalación, ESET NOD32 y ESET Smart Security contendrán 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. Desde el punto de vista de un administrador, probablemente las tareas más útiles sean **Análisis del ordenador** y **Actualizar**.

- **Análisis del ordenador**
  Proporciona un análisis periódico del antivirus (normalmente de las unidades locales) en los 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 ningún motivo para modificar sus parámetros. La única excepción son los portátiles, ya que sus propietarios se conectan a Internet a menudo 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 la actualización de los portátiles desde el servidor Mirror local, así como desde los servidores de actualización de ESET.

La configuración del Programador de Tareas también está disponible en **ESET Configuration Editor**, en ESET Smart Security / ESET NOD32 Antivirus **>** **Kernel de ESET** > **Configuración** > **Tareas programadas** > **Tareas programadas** > **Modificar**.

Para obtener más información, consulte el capítulo ESET Configuration Editor 32.



La ventana de diálogo puede contener las tareas existentes (haga clic en **Modificar** para modificarlas) o puede estar vacía. Depende de si ha abierto una configuración desde un cliente (por ejemplo, desde un cliente activo y previamente configurado) o ha abierto un archivo nuevo 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*), que se generan automáticamente al crear

una tarea nueva.

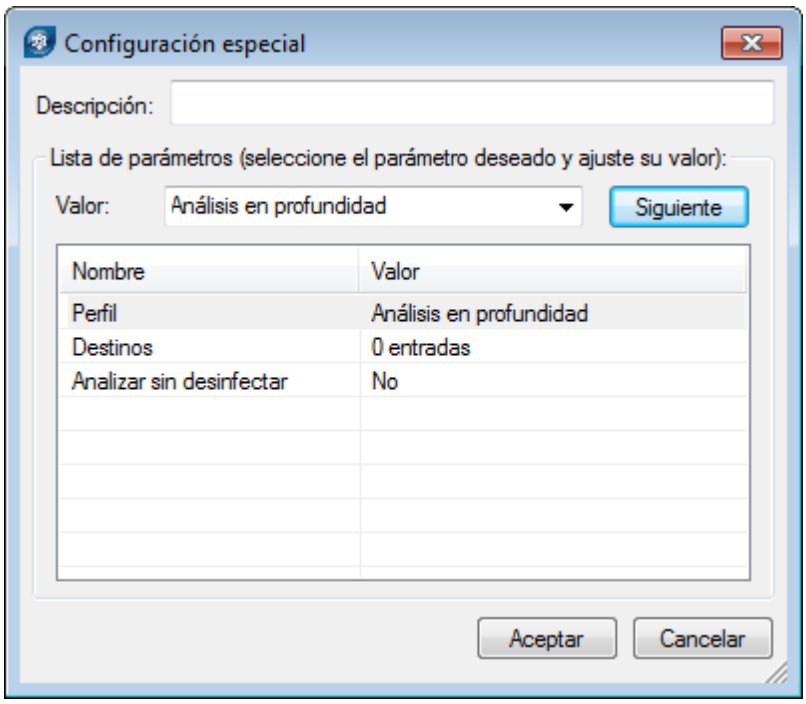
Si la casilla de verificación de una tarea está marcada, significa que dicha tarea está activa y se ejecutará en el cliente en cuestión.

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

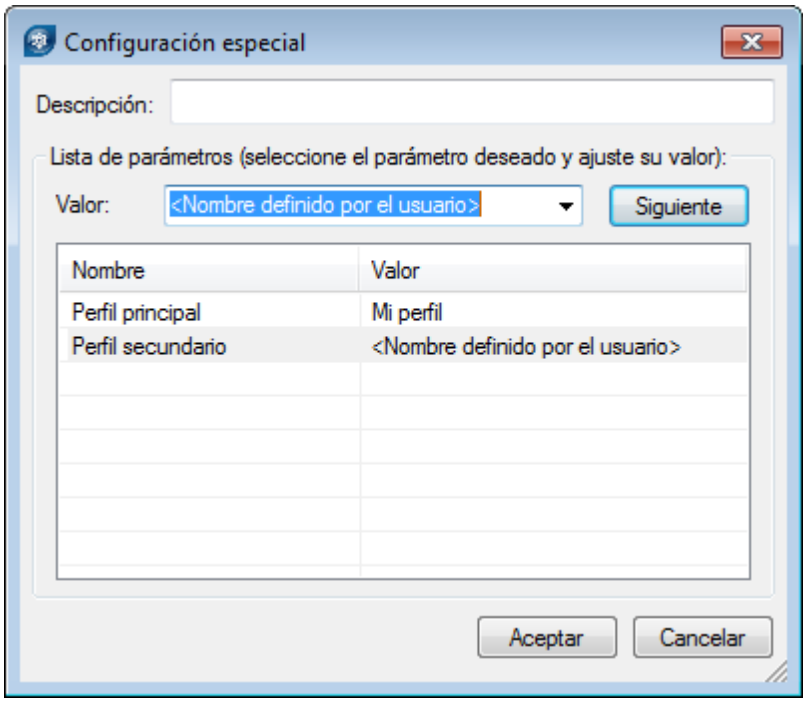
- **Agregar**: agrega una nueva tarea.
- **Modificar**: modifica las tareas seleccionadas.
- **Cambiar Id.**: modifica el Id. de las tareas seleccionadas.
- **Detalles** : muestra un resumen de la información sobre las tareas seleccionadas.
- **Marcar para eliminación**: la aplicación del archivo *.xml* eliminará las tareas (con el mismo Id.) seleccionadas al hacer clic en este botón desde los clientes de destino.
- **Quitar de la lista**: quita de la lista las tareas seleccionadas. 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 cuando edite una tarea existente (**Modificar**), debe especificar cuándo se ejecutará. La tarea se puede repetir 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 se inicie el ordenador en el día, etc.).

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



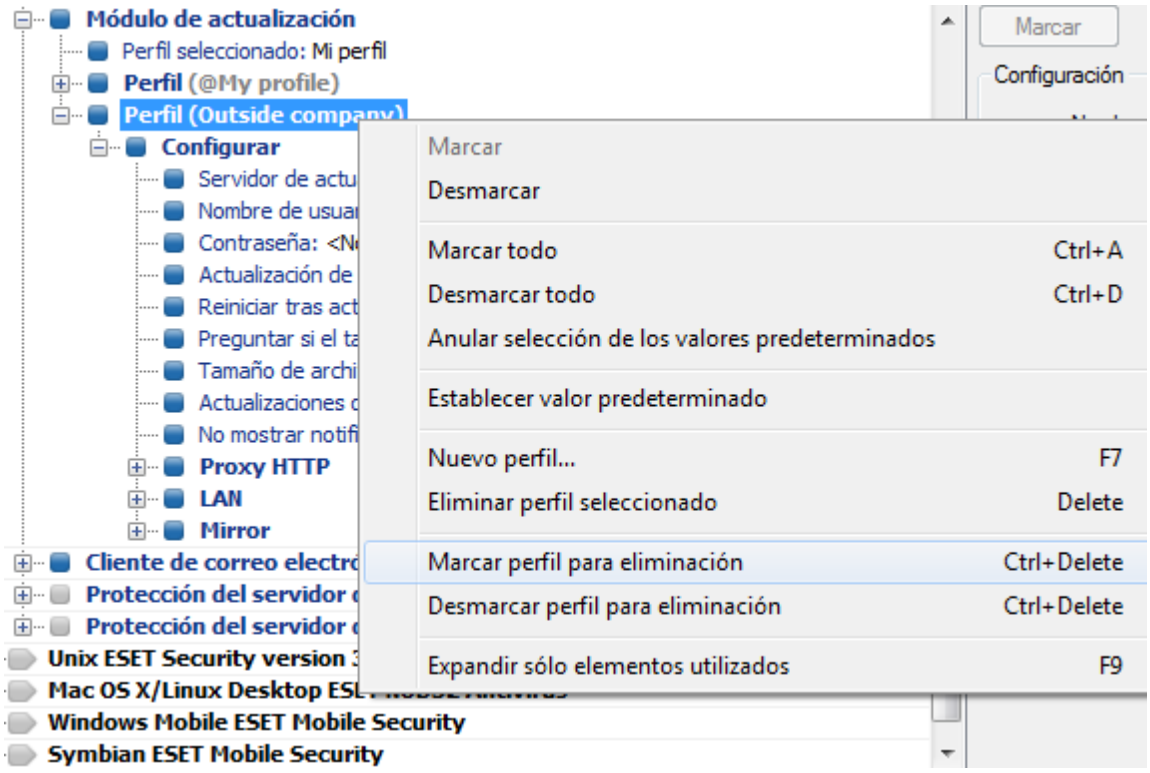
El último paso de la tarea **Actualizar** especifica los perfiles de actualización que se ejecutarán dentro de la tarea en concreto. Es una tarea predefinida y se ejecuta cada 60 minutos de forma predeterminada. Normalmente, no hay ningún motivo para modificar sus parámetros. La única excepción son los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



11.2 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:

- En ERAC, haga clic en la ficha **Clientes** y, a continuación, haga doble clic en un cliente problemático.
- En la ventana **Propiedades del cliente**, haga clic en la ficha **Configuración**. Seleccione las opciones **A continuación, ejecute ESET Configuration Editor para modificar el archivo** y **Utilice la configuración descargada en la nueva tarea de configuración**; a continuación, haga clic en el botón **Tarea nueva**.
- En el nuevo asistente de tareas, haga clic en **Modificar**.
- En Configuration Editor, pulse **CTRL+D** para anular la selección de todos los ajustes. Esto ayuda a impedir cambios accidentales, ya que todo cambio nuevo quedará destacado en azul.
- Haga clic con el botón derecho del ratón en el perfil que desea eliminar y seleccione **Marcar perfil para eliminación** en el menú contextual. El perfil se eliminará en cuanto se envíe la tarea a los clientes.



- Haga clic en el botón **Consola** de ESET Configuration Editor y guarde los ajustes.
- Compruebe que el cliente seleccionado se encuentra en la columna **Elementos seleccionados** de la derecha. Haga clic en **Siguiente** y, a continuación, en **Finalizar**.

11.3 Exportación y otras características de la configuración XML del cliente

En ERAC, seleccione clientes en la ficha **Clientes**. Haga clic con el botón derecho del ratón y seleccione **Configuración...** en el menú contextual. Haga clic en **Guardar como...** para exportar la configuración asignada del cliente a un archivo *.xml* (los archivos de configuración *.xml* también se pueden extraer directamente de la interfaz del programa ESET Smart Security). Después, podrá utilizar el archivo *.xml* para diversas operaciones:

- En instalaciones remotas, el archivo *.xml* se puede utilizar como plantilla para una configuración predefinida. De esta manera, no se crea ningún archivo *.xml* nuevo y el archivo *.xml* existente se asigna (**Seleccionar...**) a un nuevo paquete de instalación. Los archivos de la configuración *.xml* también se pueden extraer directamente desde la interfaz del programa ESET Smart Security.

- En la configuración de varios clientes, los clientes seleccionados reciben un archivo *.xml* previamente descargado y adoptan los ajustes 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 directivas"*, este método puede resultar de gran utilidad en tareas como el ajuste de las reglas del cortafuegos.

11.4 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 Mirror local. En primer lugar, los portátiles establecen conexión con el servidor Mirror y, si la conexión falla (porque se encuentren fuera del lugar de trabajo), descargan las actualizaciones directamente desde los servidores de ESET. Para permitir esta funcionalidad:

- Cree dos perfiles de actualización, Exportación y otras características de la configuración XML del cliente 95 uno destinado al servidor Mirror (llamado "LAN" en el ejemplo siguiente) y otro para los servidores de actualización de ESET (INET).

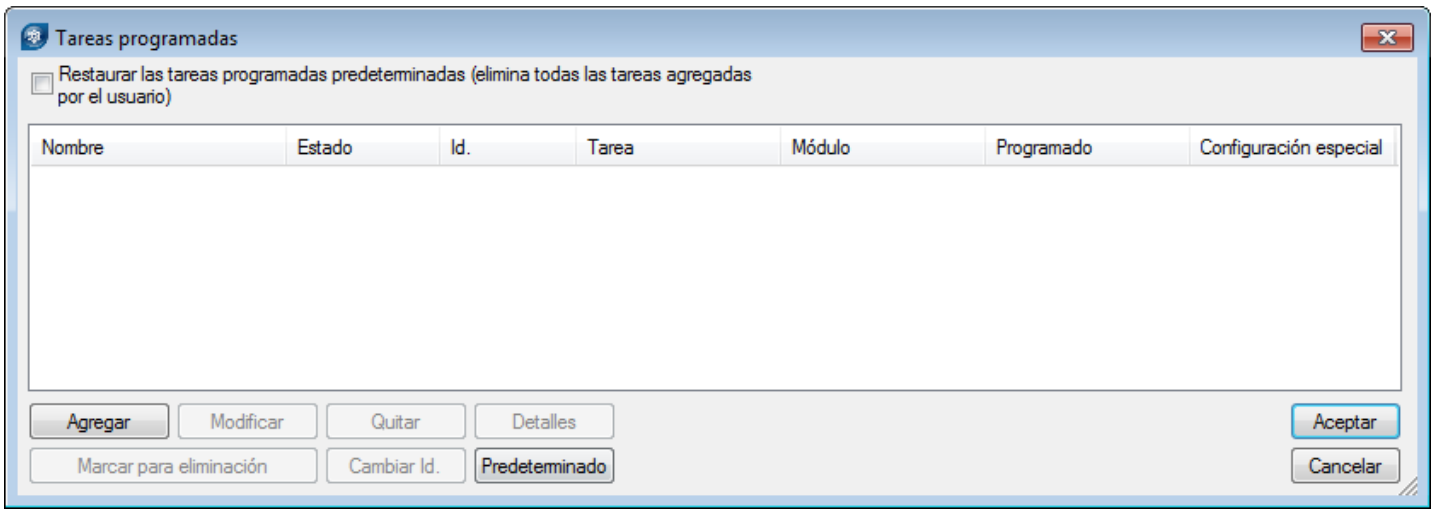
- Cree una nueva tarea de actualización o modifique una existente con el Programador de Tareas (**Herramientas** > **Programador de Tareas** en la ventana del programa principal de ESET Smart Security o ESET NOD32 Antivirus).

La configuración se puede realizar directamente desde los portátiles o de forma remota con ESET Configuration Editor. Se puede aplicar durante el proceso de instalación o más tarde como tarea de configuración.

Para crear nuevos perfiles en ESET Configuration Editor, haga clic con el botón derecho del ratón en la sección **Actualizar** y seleccione **Nuevo perfil** en el menú contextual.

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

El perfil LAN descarga actualizaciones desde el servidor Mirror local de la empresa (*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 los perfiles de actualización sucesivamente. Para hacerlo, vaya a **ESET Smart Security**, **ESET NOD32 Antivirus** > **Kernel** > **Configuración** > **Tareas programadas** en ESET Configuration Editor. Haga clic en el botón **Modificar** para abrir la ventana **Tareas programadas**.



Para crear una tarea nueva, haga clic en **Agregar**. En 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 Mirror en primer lugar, el perfil principal debería establecerse como LAN y el secundario como INET. El perfil INET sólo se aplica si falla la actualización desde LAN.

Recomendación: exporte la configuración *.xml* actual desde un cliente (para obtener más información, consulte el capítulo ¿Cómo diagnosticar problemas con ERAS? 91) y efectúe las modificaciones mencionadas en el archivo *.xml* exportado. De esta manera, se evitará toda posible duplicación entre el Programador de Tareas y los perfiles no operativos.

11.5 Instalación de productos de terceros con ERA

Además de la instalación remota de los productos de ESET, ESET Remote Administrator permite 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 capítulo Instalación remota 35.

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

1) En ERAC, haga clic en la ficha **Instalación remota**.
2) Haga clic en el botón **Paquetes**.
3) En el menú desplegable Tipo de paquete, seleccione **Paquete personalizado**.
4) Haga clic en **Agregar** y en **Agregar archivo**; a continuación, seleccione el paquete *.msi* que desee.
5) Seleccione el archivo en el menú desplegable **Archivo de entrada del paquete** y haga clic en **Crear**.
6) De vuelta en 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.
7) Haga clic en **Guardar como...** para guardar el paquete.
8) 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 consultar el procedimiento en capítulos anteriores. El paquete se puede enviar 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 ejecute el paquete.

12. ESET SysInspector

12.1 Introducción a ESET SysInspector

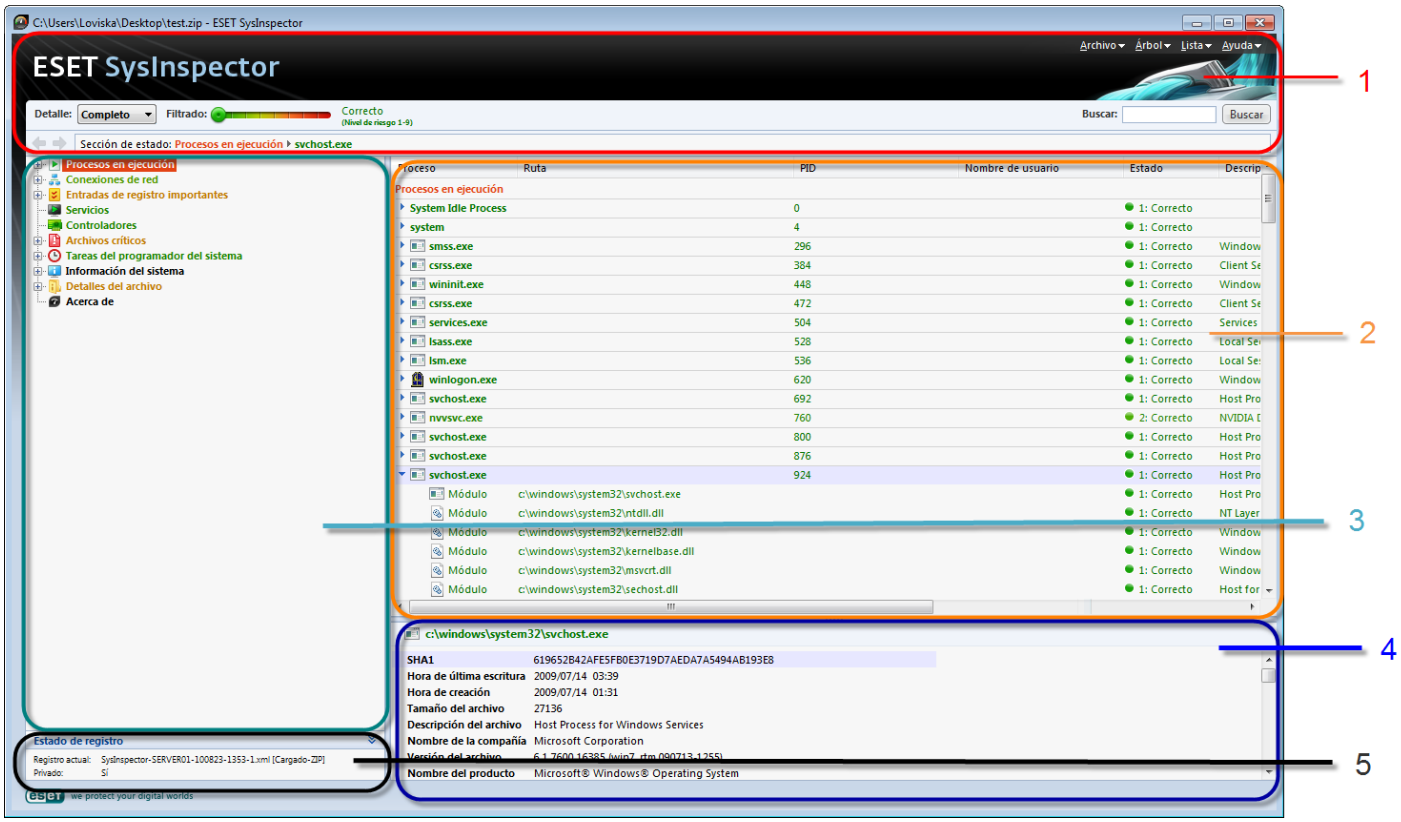
ESET SysInspector es una aplicación que examina el ordenador a fondo y muestra los datos recopilados de forma exhaustiva. La información sobre los controladores y aplicaciones instalados, las conexiones de red o las entradas de registro importantes, por ejemplo, puede ayudarle en la investigación de un comportamiento sospechoso del sistema, ya sea debido a incompatibilidades del software o hardware o a una infección por malware.

12.1.1 Inicio de ESET SysInspector

Para iniciar ESET SysInspector simplemente tiene que ejecutar el archivo *SysInspector.exe* que descargó del sitio web de ESET. Si ya tiene instalado alguno de los productos de seguridad de ESET, puede ejecutar ESET SysInspector directamente desde el menú Inicio (Programas > ESET > ...). Espere mientras la aplicación examina el sistema. El proceso de inspección puede tardar varios minutos, en función del hardware de su ordenador y de los datos que se van a recopilar.

12.2 Interfaz de usuario y uso de la aplicación

Para una administración sencilla, la ventana principal se divide en cuatro secciones principales: la sección de controles de programa (1), situada en la parte superior de la ventana principal; la ventana de navegación (3), situada a la izquierda; la ventana de descripción (2), situada en la parte central derecha; y la ventana de detalles (4), situada en la parte inferior derecha de la ventana principal. La sección Estado del registro (5) incluye los parámetros básicos de un registro (filtro utilizado, tipo de filtro, etc.) e indica si el registro es el resultado de una comparación.



12.2.1 Controles de programa

Esta sección contiene la descripción de todos los controles de programa disponibles en ESET SysInspector.

Archivo
Al hacer clic aquí, puede guardar el estado actual del sistema para examinarlo más tarde o abrir un registro guardado anteriormente. Para la publicación, es recomendable que genere un registro **Adecuado para su envío**. De esta forma, el registro omite la información confidencial (nombre del usuario actual, nombre del ordenador, nombre del dominio, privilegios del usuario actual, variables de entorno, etc.).

NOTA: Puede abrir previamente los informes de ESET SysInspector almacenados simplemente arrastrándolos y soltándolos en la ventana principal.

Árbol
Le permite expandir o cerrar todos los nodos, y exportar las secciones seleccionadas al script de servicio.

Lista
Contiene funciones para una navegación más sencilla por el programa y otras funciones como, por ejemplo, la búsqueda de información en línea.

Ayuda
Contiene información sobre la aplicación y sus funciones.

Detalle
Muestra información en otras secciones de la ventana principal, lo que facilita el uso del programa. En el modo "Básico" tiene acceso a información utilizada para buscar soluciones a problemas comunes de su sistema. En el modo "Medio", el programa muestra información menos utilizada, mientras que en el modo "Completo", ESET SysInspector muestra toda la información necesaria para solucionar problemas muy específicos.

Filtrado de elementos
Es la mejor opción para buscar entradas de registro o archivos sospechosos en el sistema. Mediante el ajuste del control deslizante, puede filtrar elementos por su nivel de riesgo. Si el control deslizante se encuentra en el extremo izquierdo (nivel de riesgo 1), se muestran todos los elementos. Al mover el control deslizante a la derecha, el programa filtra todos los elementos menos peligrosos que el nivel de riesgo actual y muestra sólo los elementos con un nivel de sospecha superior al mostrado. Si el control deslizante se encuentra en el extremo derecho, el programa muestra únicamente los elementos dañinos conocidos.

Todos los elementos pertenecientes al intervalo de riesgo comprendido entre 6 y 9 pueden suponer un riesgo para la seguridad. Si no está utilizando algunas de las soluciones de seguridad de ESET, le recomendamos que analice su sistema con ESET Online Scanner cuando el programa encuentre un elemento de este tipo. ESET Online Scanner es un servicio gratuito.

NOTA: el nivel de riesgo de un elemento se puede determinar rápidamente comparando el color del elemento con el color del control deslizante del nivel de riesgo.

Buscar
Esta opción se puede utilizar para buscar rápidamente un elemento específico por su nombre o parte del nombre. Los resultados de la solicitud de búsqueda aparecerán en la ventana de descripción.

Retorno
Al hacer clic en la flecha hacia atrás o hacia delante, puede volver a la información mostrada previamente en la ventana de descripción. Puede utilizar la tecla Retroceso y la tecla de espacio, en lugar de hacer clic en las flechas atrás y adelante.

Sección de estado
Muestra el nodo actual en la ventana de navegación.

Importante: los elementos destacados en rojo son elementos desconocidos, por eso el programa los marca como potencialmente peligrosos. Que un elemento aparezca marcado en rojo no significa que deba eliminar el archivo. Antes de eliminarlo, asegúrese de que el archivo es realmente peligroso o innecesario.

12.2.2 Navegación por ESET SysInspector

ESET SysInspector divide los tipos de información en distintas secciones básicas denominadas nodos. Si está disponible, puede encontrar información adicional expandiendo los subnodos de cada nodo. Para abrir o contraer un nodo, sólo tiene que hacer doble clic en el nombre del nodo o en ⊞ o ⊟, que se encuentran junto al nombre del nodo. Cuando examine la estructura de árbol de nodos y subnodos en la ventana de navegación, puede encontrar información variada de cada nodo en la ventana de descripción. Si examina los elementos en la ventana de descripción, es posible que se muestre información adicional de cada uno de los elementos en la ventana de detalles.

A continuación, se encuentran las descripciones de los nodos principales de la ventana de navegación e información relacionada en las ventanas de descripción y detalles.

Procesos en ejecución
Este nodo contiene información sobre aplicaciones y procesos que se ejecutan al generar el registro. En la ventana de descripción, puede encontrar información adicional de cada proceso como, por ejemplo, bibliotecas dinámicas utilizadas por el proceso y su ubicación en el sistema, el nombre del proveedor de la aplicación, el nivel de riesgo del archivo, etc.

La ventana de detalles contiene información adicional de los elementos seleccionados en la ventana de descripción como, por ejemplo, el tamaño del archivo o su hash.

NOTA: un sistema operativo incluye varios componentes del núcleo (kernel) importantes que se ejecutan de forma ininterrumpida y que proporcionan funciones básicas y esenciales para otras aplicaciones de usuario. En determinados casos, dichos procesos aparecen en la herramienta ESET SysInspector con una ruta de archivo que comienza por \??\. Estos símbolos optimizan el inicio previo de esos procesos; son seguros para el sistema y, como tal, son correctos.

Conexiones de red
La ventana de descripción contiene una lista de procesos y aplicaciones que se comunican a través de la red utilizando el protocolo seleccionado en la ventana de navegación (TCP o UDP), así como la dirección remota a la que se conecta la aplicación. También puede comprobar las direcciones IP de los servidores DNS.

La ventana de detalles contiene información adicional de los elementos seleccionados en la ventana de descripción como, por ejemplo, el tamaño del archivo o su hash.

Entradas de registro importantes
Contiene una lista de entradas de registro seleccionadas que suelen estar asociadas a varios problemas del sistema, como las que especifican programas de arranque, objetos auxiliares del navegador (BHO), etc.

En la ventana de descripción, puede encontrar los archivos que están relacionados con entradas de registro específicas. Puede ver información adicional en la ventana de detalles.

Servicios
La ventana de descripción contiene una lista de archivos registrados como Windows Services (Servicios de Windows). En la ventana de detalles, puede consultar la forma de inicio establecida para el servicio e información específica del archivo.

Controladores
Una lista de los controladores instalados en el sistema.

Archivos críticos
En la ventana de descripción se muestra el contenido de los archivos críticos relacionados con el sistema operativo Microsoft Windows.

Información del sistema
Contiene información detallada sobre el hardware y el software, así como información sobre las variables de entorno y los derechos de usuario establecidos.

Detalles del archivo
Una lista de los archivos del sistema y los archivos de la carpeta Archivos de programa importantes. Se puede encontrar información adicional específica de los archivos en las ventanas de descripción y detalles.

Acerca de
Información sobre ESET SysInspector.

12.2.3 Comparar

La característica Comparar permite al usuario comparar dos registros existentes. El resultado es un conjunto de elementos no comunes a ambos registros. Esta opción es útil para realizar un seguimiento de los cambios realizados en el sistema; le permite, por ejemplo, detectar la actividad de código malicioso.

Una vez iniciada, la aplicación crea un nuevo registro, que aparecerá en una ventana nueva. Vaya a **Archivo** -> **Guardar registro** para guardar un registro en un archivo. Los archivos de registro se pueden abrir y ver posteriormente. Para abrir un registro existente, utilice el menú **Archivo** -> **Abrir registro**. En la ventana principal del programa, ESET SysInspector muestra siempre un registro a la vez.

Si compara dos registros, el principio fundamental reside en el hecho de que compara un registro activo actualmente con un registro guardado en un archivo. Para comparar registros, utilice la opción **Archivo** -> **Comparar registros** y elija **Seleccionar archivo**. El registro seleccionado se comparará con el registro activo en la ventana principal del programa. El resultante, denominado "registro comparativo", mostrará sólo las diferencias entre esos dos registros.

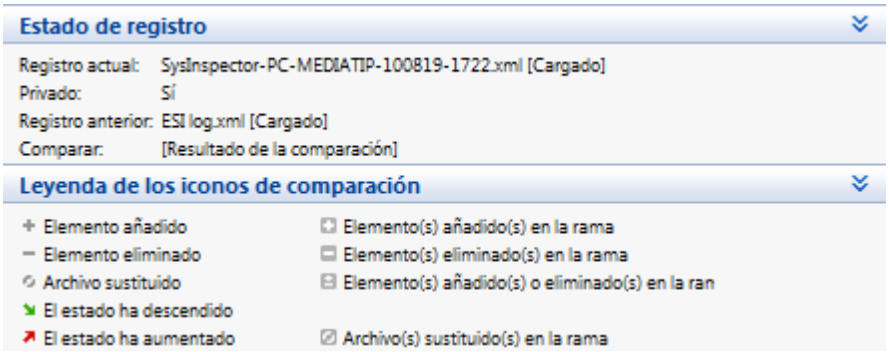
NOTA: En caso de que compare dos archivos de registro, seleccione **Archivo** -> **Guardar registro** y guárdelo como un archivo ZIP. Se guardarán ambos archivos. Si abre posteriormente dicho archivo, se compararán automáticamente los registros que contiene.

Junto a los elementos mostrados, SysInspector muestra símbolos que identifican las diferencias entre los registros comparados.
Los elementos marcados con un – sólo se encuentran en el registro activo y no están presentes en el registro comparativo abierto. Por otra parte, los elementos marcados con un + solamente están presentes en el registro abierto, no en el registro activo.

Descripción de todos los símbolos que pueden aparecer junto a los elementos:

+ Nuevo valor que no se encuentra en el registro anterior.
La sección de estructura de árbol contiene nuevos valores.
– Valor eliminado que sólo se encuentra en el registro anterior.
La sección de estructura de árbol contiene valores eliminados.
Se ha cambiado un valor o archivo.
La sección de estructura de árbol contiene valores o archivos modificados.
Ha disminuido el nivel de riesgo o era superior en el registro anterior.
Ha aumentado el nivel de riesgo o era inferior en el registro anterior.

La explicación que aparece en la esquina inferior izquierda describe todos los símbolos y muestra los nombres de los registros que se están comparando.



Se puede guardar cualquier registro comparativo en un archivo y abrirlo posteriormente.

Ejemplo:

Genere y guarde un registro, en el que se recopile información original sobre el sistema, en un archivo con el nombre "previo.xml". Tras realizar los cambios en el sistema, abra SysInspector y permita que genere un nuevo registro. Guárdelo en un archivo con el nombre *actual.xml*.
Para realizar un seguimiento de los cambios entre estos dos registros, vaya a **Archivo** -> **Comparar registros**. El programa creará un registro comparativo con las diferencias entre ambos registros.

Se puede lograr el mismo resultado si utiliza la siguiente opción de la línea de comandos:

SysIsnpector.exe actual.xml previo.xml

12.3 Parámetros de la línea de comandos

ESET SysInspector admite la generación de informes desde la línea de comandos con estos parámetros:

/gen	genera un registro directamente desde la línea de comandos, sin ejecutar la interfaz gráfica de usuario
/privacy	genera un registro en el que se excluye la información confidencial
/zip	almacena el registro resultante directamente en el disco, en un archivo comprimido
/silent	oculta la barra de progreso del proceso de generación del registro
/help, **/?**	muestra información acerca de los parámetros de la línea de comandos

Ejemplos

Para cargar un registro determinado directamente en el navegador, utilice: *SysInspector.exe "c:\clientlog.xml"*
Para generar un registro en una ubicación actual, utilice: *SysInspector.exe /gen*
Para generar un registro en una carpeta específica, utilice: *SysInspector.exe /gen="c:\folder\"*
Para generar un registro en una carpeta o ubicación específica, utilice: *SysInspector.exe /gen="c:\folder\mynewlog.xml"*
Para generar un registro en el que se excluya la información confidencial directamente como archivo comprimido, utilice: *SysInspector.exe /gen="c:\mynewlog.zip" /privacy /zip*
Para comparar dos registros, utilice: *SysInspector.exe "actual.xml" "original.xml"*

NOTA: si el nombre del archivo o la carpeta contiene un espacio, debe escribirse entre comillas.

12.4 Script de servicio

El script de servicio es una herramienta que ofrece asistencia a los clientes que utilizan ESET SysInspector. Sirve para eliminar objetos no deseados del sistema.

El script de servicio permite al usuario exportar el registro completo de SysInspector o únicamente las partes seleccionadas. Tras la exportación, puede marcar los objetos que desee eliminar. A continuación, puede ejecutar el registro modificado para eliminar los objetos marcados.

El script de servicio es útil para usuarios avanzados con experiencia previa en el diagnóstico de problemas del sistema. Las modificaciones realizadas por usuarios sin experiencia pueden impedir el funcionamiento del sistema operativo.

Ejemplo:

Si tiene la sospecha de que el ordenador está infectado por un virus que el antivirus no detecta, siga las instrucciones siguientes:

- Ejecute ESET SysInspector para generar una nueva instantánea del sistema.
- Seleccione el primer elemento de la sección que se encuentra a la izquierda (en la estructura de árbol), pulse Ctrl y seleccione el último elemento para marcarlos todos. Suelte la tecla Ctrl.
- Haga clic con el botón secundario en los objetos seleccionados y elija la opción **Exportar las secciones seleccionadas al script de servicio** en el menú contextual.
- Los objetos seleccionados se exportarán a un nuevo registro.
- Este es el paso más importante de todo el procedimiento: abra el registro nuevo y cambie el atributo - a + para todos los objetos que desee eliminar. Asegúrese de no marcar ninguno de los objetos necesarios para el correcto funcionamiento del sistema.
- Abra ESET SysInspector, haga clic en **Archivo** > **Ejecutar script de servicio** e introduzca la ruta del script.
- Haga clic en **Aceptar** para ejecutar el script

12.4.1 Generación de scripts de servicio

Para generar un script de servicio, haga clic con el botón secundario en cualquier elemento del árbol de menús (en el panel izquierdo) de la ventana principal de SysInspector. En el menú contextual, seleccione la opción **Exportar todas las secciones al script de servicio** o la opción **Exportar las secciones seleccionadas al script de servicio**.

NOTA: cuando se comparan dos registros, el script de servicio no se puede exportar.

12.4.2 Estructura del script de servicio

En la primera línea del encabezado del script encontrará información sobre la versión del motor (ev), la versión de la interfaz gráfica de usuario (gv) y la versión del registro (lv). Puede utilizar estos datos para realizar un seguimiento de los posibles cambios del archivo .xml que genere el script y evitar las incoherencias durante la ejecución. Esta parte del script no se debe modificar.

El resto del archivo se divide en secciones, donde los elementos se pueden modificar (indique los que procesará el script). Para marcar los elementos que desea procesar, sustituya el carácter "-" situado delante de un elemento por el carácter "+". En el script, las secciones se separan mediante una línea vacía. Cada sección tiene un número y un título.

01) Running processes (Procesos en ejecución)

En esta sección se incluye una lista de todos los procesos que se están ejecutando en el sistema. Cada proceso se identifica mediante su ruta UNC y, posteriormente, su código hash CRC16 representado mediante asteriscos (*).

Ejemplo:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

En este ejemplo se ha seleccionado (marcado con el carácter "+") el proceso module32.exe, que finalizará al ejecutar el script.

02) Loaded modules (Módulos cargados)

En esta sección se listan los módulos del sistema que se utilizan actualmente.

Ejemplo:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

En este ejemplo, se marcó el módulo khbekhb.dll con el signo "+". Cuando se ejecute, el script reconocerá los procesos mediante el módulo específico y los finalizará.

03) TCP connections (Conexiones TCP)

En esta sección se incluye información sobre las conexiones TCP existentes.

Ejemplo:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

Cuando se ejecute, el script localizará al propietario del socket en las conexiones TCP marcadas y detendrá el socket,

liberando así recursos del sistema.

04) UDP endpoints (Puntos finales UDP)

En esta sección se incluye información sobre los puntos finales UDP.

Ejemplo:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Cuando se ejecute, el script aislará al propietario del socket en los puntos finales UDP marcados y detendrá el socket.

05) DNS server entries (Entradas del servidor DNS)

En esta sección se proporciona información sobre la configuración actual del servidor DNS.

Ejemplo:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Las entradas marcadas del servidor DNS se eliminarán al ejecutar el script.

06) Important registry entries (Entradas de registro importantes)

En esta sección se proporciona información sobre las entradas de registro importantes.

Ejemplo:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

Cuando se ejecute el script, las entradas marcadas se eliminarán, reducirán a valores de 0 bytes o restablecerán en sus valores predeterminados. La acción realizada en cada entrada depende de su categoría y del valor de la clave en el registro específico.

07) Services (Servicios)

En esta sección se listan los servicios registrados en el sistema.

Ejemplo:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

Cuando se ejecute el script, los servicios marcados y los servicios dependientes se detendrán y desinstalarán.

08) Drivers (Controladores)

En esta sección se listan los controladores instalados.

Ejemplo:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Cuando se ejecuta el script, se anula el registro del sistema de los controladores seleccionados, que después se eliminan.

09) Critical files (Archivos críticos)

En esta sección se proporciona información sobre los archivos críticos para el correcto funcionamiento del sistema operativo.

Ejemplo:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[…]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[…]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[…]
```

Los elementos seleccionados se eliminarán o restablecerán en sus valores originales.

12.4.3 Ejecución de scripts de servicio

Seleccione todos los elementos que desee y, a continuación, guarde y cierre el script. Ejecute el script modificado directamente desde la ventana principal de SysInspector, con la opción Ejecutar el script de servicio del menú Archivo. Cuando abra un script, el programa mostrará el mensaje siguiente: **¿Está seguro de que desea ejecutar el script de servicio "%Scriptname%"?** Una vez que haya confirmado la selección, es posible que se muestre otra advertencia para informarle de que el script de servicio que intenta ejecutar no está firmado. Haga clic en **Ejecutar** para iniciar el script.

Se mostrará una ventana de diálogo para confirmar la correcta ejecución del script.

Si el script no se puede procesar por completo, se mostrará una ventana de diálogo con el mensaje siguiente: **El script de servicio se ejecutó parcialmente. ¿Desea ver el informe de errores?** Seleccione **Sí** para ver un informe de errores completo con todas las operaciones que no se ejecutaron.

Si no se reconoce el script, aparece una ventana de diálogo con el mensaje siguiente: **No se ha firmado el script de servicio seleccionado. La ejecución de scripts desconocidos y sin firmar podría dañar seriamente los datos del ordenador. ¿Está seguro de que desea ejecutar el script y llevar a cabo las acciones?** Esto podría deberse a que el script presenta inconsistencias (encabezado dañado, título de sección dañado, falta línea vacía entre secciones, etc.). Vuelva a abrir el archivo del script y corrija los errores o cree un script de servicio nueva.

12.5 Accesos directos

Los accesos directos que se pueden utilizar en ESET SysInspector son:

Archivo

Ctrl+O	Abrir el registro existente
Ctrl+S	Guardar los registros creados

Generar

Ctrl+G	Comprobación estándar del estado del sistema
Ctrl+H	Realizar una comprobación del sistema que también puede registrar información confidencial

Filtrado de elementos

1, O	Seguro, se muestran los elementos que tienen un nivel de riesgo de 1 a 9.
2	Seguro, se muestran los elementos que tienen un nivel de riesgo de 2 a 9.
3	Seguro, se muestran los elementos que tienen un nivel de riesgo de 3 a 9.
4, U	Desconocido, se muestran los elementos que tienen un nivel de riesgo de 4 a 9.
5	Desconocido, se muestran los elementos que tienen un nivel de riesgo de 5 a 9.
6	Desconocido, se muestran los elementos que tienen un nivel de riesgo de 6 a 9.
7, B	Peligroso, se muestran los elementos que tienen un nivel de riesgo de 7 a 9.
8	Peligroso, se muestran los elementos que tienen un nivel de riesgo de 8 a 9.
9	Peligroso, se muestran los elementos que tienen un nivel de riesgo de 9.
-	Disminuir el nivel de riesgo
+	Aumentar el nivel de riesgo
Ctrl+9	Modo de filtrado, mismo nivel o superior
Ctrl+0	Modo de filtrado, sólo mismo nivel

Ver

Ctrl+5	Ver por proveedor, todos los proveedores
Ctrl+6	Ver por proveedor, sólo Microsoft
Ctrl+7	Ver por proveedor, resto de proveedores
Ctrl+3	Mostrar todos los detalles
Ctrl+2	Mostrar la mitad de los detalles
Ctrl+1	Visualización básica
Retroceso	Volver un paso atrás
Espacio	Continuar con el paso siguiente
Ctrl+W	Expandir el árbol
Ctrl+Q	Contraer el árbol

Otros controles

Ctrl+T	Ir a la ubicación original del elemento tras seleccionarlo en los resultados de búsqueda
Ctrl+P	Mostrar la información básica de un elemento
Ctrl+A	Mostrar la información completa de un elemento
Ctrl+C	Copiar el árbol del elemento actual
Ctrl+X	Copiar elementos
Ctrl+B	Buscar información en Internet acerca de los archivos seleccionados
Ctrl+L	Abrir la carpeta en la que se encuentra el archivo seleccionado
Ctrl+R	Abrir la entrada correspondiente en el editor de registros
Ctrl+Z	Copiar una ruta de acceso a un archivo (si el elemento está asociado a un archivo)
Ctrl+F	Activar el campo de búsqueda
Ctrl+D	Cerrar los resultados de búsqueda
Ctrl+E	Ejecutar el script de servicio

Comparación

Ctrl+Alt+O	Abrir el registro original/comparativo
Ctrl+Alt+R	Cancelar la comparación
Ctrl+Alt+1	Mostrar todos los elementos
Ctrl+Alt+2	Mostrar sólo los elementos agregados, el registro incluirá los elementos presentes en el registro actual
Ctrl+Alt+3	Mostrar sólo los elementos eliminados, el registro incluirá los elementos presentes en el registro anterior
Ctrl+Alt+4	Mostrar sólo los elementos sustituidos (archivos incluidos)
Ctrl+Alt+5	Mostrar sólo las diferencias entre los registros
Ctrl+Alt+C	Mostrar la comparación
Ctrl+Alt+N	Mostrar el registro actual
Ctrl+Alt+P	Abrir el registro anterior

Varios

F1	Ver la Ayuda
Alt+F4	Cerrar el programa
Alt+Mayús+F4	Cerrar el programa sin preguntar
Ctrl+I	Estadísticas del registro

12.6 Requisitos del sistema

Para un funcionamiento óptimo de ESET SysInspector, el sistema debería cumplir con los siguientes requisitos de hardware y software::

Windows 2000, XP, 2003
400 MHz 32 bits (x86)/64 bits (x64)
128MB RAM de memoria del sistema
10 MB de espacio disponible
Super VGA (800 x 600)

Windows 7, Vista, 2008
1 GHz 32 bits (x86)/64 bits (x64)
512 MB RAM de memoria del sistema
10 MB de espacio disponible
Super VGA (800 x 600)

12.7 Preguntas frecuentes

¿Es necesario contar con privilegios de administrador para ejecutar ESET SysInspector?

ESET SysInspector no requiere privilegios de administrador para su ejecución, sí es necesario utilizar una cuenta de administrador para acceder a parte de la información que recopila. Si lo ejecuta como usuario normal o restringido, se recopilará menor cantidad de información acerca de su entorno operativo.

¿ESET SysInspector crea archivos de registro?

ESET SysInspector puede crear un archivo de registro de la configuración de su ordenador. Para guardarlo, seleccione Archivo > Guardar registro en el menú principal. Los registros se guardar con formato XML. De forma predeterminada, los archivos se guardan en el directorio %USERPROFILE%\Mis documentos\, con una convención de nomenclatura del tipo "SysInpsector-%COMPUTERNAME%-AAMMDD-HHMM.XML". Si lo desea, puede modificar tanto la ubicación como el nombre del archivo de registro antes de guardarlo.

¿Cómo puedo ver el contenido del archivo de registro de ESET SysInspector?

Para visualizar un archivo de registro creado por ESET SysInspector, ejecute la aplicación y seleccione Archivo > Abrir registro en el menú principal. También puede arrastrar y soltar los archivos de registro en la aplicación ESET SysInspector. Si necesita ver los archivos de registro de ESET SysInspector con frecuencia, le recomendamos que cree un acceso directo al archivo SYSINSPECTOR.EXE en su escritorio. Para ver los archivos de registro, arrástrelos y suéltelos en ese acceso directo. Por razones de seguridad, es posible que Windows Vista no permita la acción de arrastrar y soltar entre ventanas que cuentan con permisos de seguridad diferentes.

¿Existe alguna especificación disponible para el formato del archivo de registro? ¿Y algún conjunto de herramientas para el desarrollo de aplicaciones (SDK)?

Actualmente, no se encuentra disponible ninguna especificación para el formato del archivo de registro, ni un conjunto de herramientas de programación, ya que la aplicación se encuentra aún en fase de desarrollo. Una vez que se haya lanzado, podremos proporcionar estos elementos en función de la demanda y los comentarios por parte de los clientes.

¿Cómo evalúa ESET SysInspector el riesgo que plantea un objeto en particular?

Generalmente, ESET SysInspector asigna un nivel de riesgo a los objetos (archivos, procesos, claves de registro, etc). Para esto, utiliza una serie de reglas heurísticas que examinan las características de cada uno de ellos y después estima el potencial de actividad maliciosa. Según estas heurísticas, a los objetos se les asignará un nivel de riesgo desde el valor "1: seguro" (en color verde) hasta "9: peligroso" (en color rojo). En el panel de navegación que se encuentra a la izquierda, las secciones estarán coloreadas según el nivel máximo de peligrosidad que presente un objeto en su interior.

El nivel de riesgo "6: desconocido (en color rojo)", ¿significa que un objeto es peligroso?

Las evaluaciones de ESET SysInspector no garantizan que un objeto sea malicioso. Esta determinación deberá confirmarla un experto en seguridad informática. ESET SysInspector está diseñado para proporcionar una guía rápida a estos expertos, con la finalidad de que conozcan los objetos que deberían examinar en un sistema en busca de algún comportamiento inusual.

¿Por qué ESET SysInspector se conecta a Internet cuando se ejecuta?

Como muchas otras aplicaciones, ESET SysInspector contiene una firma digital que actúa a modo de "certificado". Esta firma sirve para garantizar que ESET ha desarrollado la aplicación y que no se ha alterado. Para comprobar la autenticidad del certificado, el sistema operativo debe contactar con la autoridad certificadora, que verificará la identidad del desarrollador de la aplicación. Este es un comportamiento normal para todos los programas firmados digitalmente que se ejecutan en Microsoft Windows.

¿En qué consiste la tecnología Anti Stealth?

La tecnología Anti Stealth proporciona un método efectivo de detección de programas peligrosos.
Si código malicioso que se comporta como un rootkit ataca al sistema, el usuario se expone a riesgos por daños, pérdidas o robo de información. Si no se dispone de una herramienta anti-rootkit especial, es prácticamente imposible detectar los rootkits.

¿Por qué a veces hay archivos con la marca "Firmado por MS" que, al mismo tiempo, tienen una entrada de "Nombre de compañía" diferente?

Al intentar identificar la firma digital de un archivo ejecutable, SysInspector comprueba en primer lugar si el archivo contiene una firma digital integrada. En ese caso, esa identificación del archivo será la que se utilice a la hora de validarlo. Por otro lado, en caso de que el archivo no contenga ninguna firma digital, ESI comienza a buscar el archivo CAT correspondiente (Catálogo de seguridad: %systemroot%\system32\catroot). Si el archivo CAT no se encuentra, la firma digital de dicho archivo CAT será la que se aplique en el proceso de validación del archivo ejecutable.

Esa es la razón por la cual a veces hay archivos marcados como "Firmado por MS", pero que tienen una entrada "Nombre de compañía" diferente.

Ejemplo:

Windows 2000 incluye la aplicación HyperTerminal, que se encuentra en *C:\Archivos de programa\Windows NT*. El archivo ejecutable de la aplicación principal no está firmado digitalmente; sin embargo, SysInspector lo marca como archivo firmado por Microsoft. La razón es la referencia que aparece en *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* que lleva a *C:\Archivos de programa\Windows NT\hypertrm.exe* (archivo ejecutable principal de la aplicación HyperTerminal), y *sp4.cat* está digitalmente firmado por Microsoft.

13. ESET SysRescue

ESET SysRescue es una utilidad que le permite crear un disco de arranque que contenga ESET NOD32 Antivirus (EAV) o ESET Smart Security (ESS). La ventaja principal de ESET SysRescue es que, aun teniendo un acceso directo al disco y a todo el sistema de archivos, tanto ESS como EAV se pueden ejecutar con independencia del sistema operativo host. Gracias a esto, es posible eliminar las infecciones que normalmente no se podrían suprimir como, por ejemplo, cuando el sistema operativo se está ejecutando.

13.1 Requisitos mínimos

ESET SysRescue funciona en el entorno de preinstalación de Microsoft Windows (Windows PE) versión 2.x, que se basa en Windows Vista. Windows PE forma parte del paquete gratuito Kit de instalación automatizada de Windows (AIK de Windows), que debe instalarse previamente para poder crear ESET SysRescue (http://www.microsoft.com/Downloads/details.aspx?familyid=94BB6E34-D890-4932-81A5-5B50C657DE08&displaylang=en). Debido a la compatibilidad con la versión de 32 bits de Windows PE, es necesario utilizar un paquete de instalación de ESS/EAV de 32 bits para la creación de ESET SysRescue en sistemas de 64 bits. ESET SysRescue es compatible con AIK de Windows 1.1 y versiones posteriores. ESET SysRescue está disponible en ESS/EAV 4.0 y versiones posteriores.

Sistemas operativos compatibles:

- Windows 7
- Windows Vista
- Windows Vista Service Pack 1
- Windows Server 2008
- Windows Server 2003 Service Pack 1 con KB926044
- Windows Server 2003 Service Pack 2
- Windows XP Service Pack 2 con KB926044

13.2 Cómo crear un CD de recuperación

Si se cumplen los requisitos mínimos para la creación de un CD de ESET SysRescue, se trata de una tarea fácil de llevar a cabo. Para iniciar el asistente de ESET SysRescue, haga clic en **Inicio** > **Programas** > **ESET** > **ESET NOD32 Antivirus** > **ESET SysRescue**.

En primer lugar, el asistente comprueba la presencia del AIK de Windows y de un dispositivo adecuado para la creación del medio de arranque.

En el siguiente paso, seleccione el medio de destino donde se ubicará ESET SysRescue . Además de CD, DVD y USB, puede elegir guardar el ESET SysRescue en un archivo ISO. Después, puede grabar esta imagen ISO en un CD o DVD, o bien usarla de algún otro modo (p. ej., en un entorno virtual como VMware o Virtualbox).

Cuando haya especificado todos los parámetros, verá una vista previa de la compilación en el último paso del asistente de ESET SysRescue. Compruebe los parámetros e inicie la compilación. Entre las opciones disponibles están:

Carpetas 109
ESET Antivirus 110
Avanzadas 110
Dispositivo USB de arranque 110
Grabación 110

13.2.1 Carpetas

Carpeta temporal es un directorio de trabajo que contiene los archivos necesarios durante la compilación de ESET SysRescue.

La carpeta **ISO** es la carpeta donde se guarda el archivo ISO resultante una vez completada la compilación.

En la lista de esta ficha se muestran todas las unidades de red locales y asignadas, así como el espacio libre disponible. Si alguna de las carpetas está en una unidad con poco espacio libre, le recomendamos que seleccione otra unidad con más espacio disponible. De lo contrario, la compilación puede finalizar antes de tiempo por falta de espacio libre en el disco.

13.2.2 ESET Antivirus

Para crear un CD de ESET SysRescue, puede seleccionar dos fuentes de archivos ESET para la compilación.

Carpeta de ESS: archivos que ya se encuentran en la carpeta del ordenador donde se ha instalado el producto de ESET.
Archivo MSI: se utilizan los archivos que se encuentran en el instalador de MSI.
Perfil: puede utilizar una de las fuentes de nombre de usuario y contraseña que aparecen a continuación:
ESS instalado: el nombre de usuario y la contraseña se copian desde la edición instalada actualmente de ESET Smart Security o ESET NOD32 Antivirus.
Del usuario: se utilizan el nombre de usuario y la contraseña introducidos en los cuadros de texto correspondientes.

NOTA: el antivirus ESET Smart Security o ESET NOD32 Antivirus presentes en el CD de ESET SysRescue se actualizan a través de Internet o mediante la solución ESET Security instalada en el ordenador donde se ejecuta el CD de ESET SysRescue.

13.2.3 Configuración avanzada

En la ficha **Avanzadas**, puede optimizar el CD de ESET SysRescue en función de la cantidad de memoria del ordenador. Seleccione **512 MB o más** para escribir el contenido del CD en la memoria operativa (RAM). Si selecciona **menos de 512 MB**, se obtendrá acceso temporalmente al CD de recuperación durante la ejecución de WinPE.

Controladores externos: en esta sección puede insertar controladores para su hardware específico (normalmente, un adaptador de red). Aunque WinPE se basa en Windows Vista SP1, que admite un amplio abanico de sistemas de hardware, a veces no reconoce el hadware y debe agregar el controlador manualmente. Hay dos maneras de agregar el controlador a la compilación de ESET SysRescue: manualmente (con el botón **Agregar**) y de forma automática (con el botón **Búsq. auto.**). Si lo agrega manualmente, debe seleccionar la ruta de acceso al archivo .inf correspondiente (el archivo *.sys aplicable también debe estar presente en esta carpeta). Si lo agrega automáticamente, el controlador se busca de forma automática en el sistema operativo del ordenador en cuestión. La adición automática se recomienda únicamente cuando ESET SysRescue se utiliza en un ordenador que tiene el mismo adaptador de red que el ordenador con el que se creó el CD de ESET SysRescue. Cuando se crea el CD de ESET SysRescue, el controlador se incluye en la compilación, de forma que el usuario no tiene que buscarlo posteriormente.

13.2.4 Dispositivo USB de arranque

Si ha seleccionado un dispositivo USB como medio de destino, puede seleccionar uno de los medios USB disponibles en la ficha **Dispositivo USB de arranque** (en caso de que haya más dispositivos USB).

13.2.5 Grabar

Si ha seleccionado CD/DVD como medio de destino, puede especificar los parámetros de grabación adicionales en la ficha Grabar.

Eliminar archivo ISO: marque esta opción para eliminar los archivos ISO una vez que se haya creado el CD de ESET SysRescue.
Eliminación activada: permite seleccionar entre borrado rápido y completo.
Dispositivo de grabación: seleccione la unidad que se utilizará para grabar.

Alerta: esta es la opción predeterminada. Si se utiliza un CD/DVD regrabable, se borrarán todos los datos contenidos en dicho CD/DVD.

La sección Medio contiene información sobre el medio introducido en el dispositivo de CD/DVD.

Velocidad de grabación: seleccione la velocidad deseada en el menú desplegable. Las capacidades de su dispositivo de grabación y el tipo de CD/DVD utilizado deben tenerse en cuenta a la hora de seleccionar la velocidad de grabación.

13.3 Trabajo con ESET SysRescue

Para que el CD/DVD/USB de recuperación funcione eficazmente, debe iniciar el ordenador desde el medio de arranque de ESET SysRescue. La prioridad de arranque puede modificarse en la BIOS. También puede ejecutar el menú de arranque durante el inicio del ordenador; normalmente, esto se hace con la tecla F9 o F12, en función de la versión de la placa base/BIOS que utilice.

ESS/EAV se iniciará cuando el sistema se haya arrancado. ESET SysRescue se utiliza únicamente en situaciones específicas, por lo que algunos módulos de protección y características del programa incluidos en ESS/EAV no son necesarios; los módulos se reducen a **Análisis del ordenador**, **Actualizar** y algunas secciones de **Configuración**. La característica más importante de ESET SysRescue es la capacidad para actualizar la base de firmas de virus. Le recomendamos que actualice el programa antes de iniciar un análisis del ordenador.

13.3.1 Uso de ESET SysRescue

Supongamos que hay ordenadores de la red que están infectados por un virus que modifica los archivos ejecutables (EXE). ESS/EAV es capaz de desinfectar todos los archivos infectados, excepto explorer.exe, que no se puede desinfectar ni en modo a prueba de errores.
Explorer.exe, como uno de los procesos esenciales de Windows, se inicia también en el modo a prueba de errores. ESS/EAV no puede realizar ninguna acción en el archivo y, por lo tanto, este sigue infectado.
En esta situación, puede emplear ESET SysRescue para solucionar el problema. ESET SysRescue no necesita ningún componente del sistema operativo host. Por tanto, es capaz de procesar (desinfectar, eliminar) todos los archivos del disco.