ThinkVantage

Guía de despliegue de Tecnologías ThinkVantage

Actualizada: 13 Octubre 2005

Incluye:

- Rescue and Recovery Versión 3.0
- Client Security Solution Versión 6.0
- Software de huellas dactilares Versión 4.6

ThinkVantage

Guía de despliegue de Tecnologías ThinkVantage

Actualizada: 13 Octubre 2005

Primera edición (setiembre de 2005)

Este manual es la traducción del original inglés *ThinkVantage Technologies Deployment Guide*.

Contenido

Prefacio

Esta guía está destinada a los administradores de TI, o a aquellos que sean responsables del despliegue del programa Rescue and Recovery en los sistemas de sus empresas. El objetivo de Rescue and Recovery es reducir costes evitando las llamadas al Helpdesk y visitas a los escritorios, así como mejorar la productividad del usuario. Es una herramientas esencial que permite a los usuarios y a los administradores restaurar copias de seguridad, acceder a archivos, diagnosticar problemas y realizar conexiones Ethernet en caso de que el sistema operativo Microsoft® Windows no se abra o no se ejecute correctamente. También permite el despliegue de actualizaciones críticas en sistemas que están corruptos o fuera de la red, así como la aplicación automática de parches al sistema cuando se realiza una restauración. Esta guía proporciona la información necesaria para instalar la aplicación Rescue and Recovery en uno o varios sistemas, siempre que estén disponibles licencias del software para cada sistema de destino, así como la información sobre los muchos aspectos de las herramientas que se pueden personalizar para dar soporte a las políticas de TI o de la empresa. Para preguntas e información acerca de la utilización de los varios componentes incluidos en el espacio de trabajo de Rescue and Recovery, consulte el sistema de ayuda en línea para los componentes.

Rescue and Recovery proporciona ayuda sobre las funciones y las aplicaciones. Para preguntas e información acerca de la utilización de los varios componentes incluidos en el espacio de trabajo de Rescue and Recovery, consulte el sistema de ayuda en línea para los componentes.

Esta guía de despliegue ha sido desarrollada teniendo en cuenta a los profesionales de TI y los retos exclusivos a los que éstos se enfrentan. Si tiene sugerencias o comentarios, póngase en contacto con el representante autorizado de Lenovo. Estas guías se actualizan periódicamentes, por lo que debe comprobar el sitio Web para obtener las versiones más recientes:

www.lenovo.com/ThinkVantage

Capítulo 1. Visión general

Las personas a las que está destinada esta guía son el personal de TI de seguridad, administración y otros responsables de la implementación y el despliegue de la tecnología de seguridad en una empresa. ThinkVantage Rescue and Recovery representa una combinación única de tecnologías de ThinkVantage. Esta aplicación integrada proporciona una suite de potentes herramientas que se pueden utilizar si no se inicia el sistema operativo Microsoft Windows.

En el entorno de una empresa, estas tecnologías pueden ayudar directa e indirectamente a los profesionales de TI. Todas las tecnologías de ThinkVantage pueden beneficiar a los profesionales de TI porque hacen que la utilización de los sistemas personales sea más fácil, más autosuficiente y proporcionan potentes herramientas que facilitan y simplifican las rotaciones. De forma continuada, las tecnologías ThinkVantage ayudan a los profesionales de TI a emplear menos tiempo solucionando problemas de sistemas individuales y más tiempo dedicados a sus tareas principales.

Componentes principales

Los componentes principales de esta guía son:

- ThinkVantage Rescue and Recovery
- ThinkVantage Client Security Solution
- Software de huellas dactilares de ThinkVantage

A continuación se presenta una descripción de cada uno de ellos.

Rescue and Recovery

Rescue and Recovery tiene dos componentes principales:

- El entorno del Área previa al escritorio de Rescue and Recovery se inicia incluso si no se arranca el sistema operativo Windows.
- El entorno de Windows de Rescue and Recovery le permite realizar copias de seguridad, rescatar archivos y recuperar el sistema operativo y los archivos.

Nota: Algunas características de Rescue and Recovery se ejecutan en el sistema operativo Windows. En algunos casos, la información del sistema utilizada en el entorno de Rescue and Recovery se recopila mientras se está ejecutando Windows. Si el sistema operativo Windows funciona incorrectamente, ese funcionamiento incorrecto solamente no impedirá que el entorno de Rescue and Recovery funcione normalmente. Sin embargo, las funciones que se ejecutan en el sistema operativo Windows no son configurables y, por lo tanto, estas funciones no se tratan en esta guía de despliegue.

Entorno del Área previa al escritorio de Rescue and Recovery

El entorno de Rescue and Recovery proporciona un espacio de trabajo de emergencia para los usuarios finales que no pueden iniciar Windows en sus sistemas. Ejecutándose en el entorno de preinstalación de Windows, el entorno ofrece el aspecto y la funcionalidad de Windows y ayuda a los usuarios a solucionar problemas sin consumir tiempo del personal de TI.

El entorno de Rescue and Recovery tiene cuatro categorías principales de funciones:

- **Rescatar y restaurar**
  - **Visión general de la recuperación:** Enlaza a los usuarios con temas de ayuda acerca de las diferentes opciones de recuperación que se proporcionan.
  - **Rescatar archivos:** Permite a los usuarios copiar archivos creados en aplicaciones de Windows en soportes extraíbles o en una red, y continuar trabajando incluso con una estación de trabajo inhabilitada.
  - **Restaurar a partir de una copia de seguridad:** Permite a los usuarios restaurar archivos de los que se ha realizado una copia de seguridad mediante Rescue and Recovery.
- **Configurar**
  - **Visión general de la configuración:** Enlaza con los temas de ayuda del entorno de Rescue and Recovery que tratan sobre la configuración.
  - **Recuperar frase de paso/contraseña:** Proporciona a un usuario o a un administrador la posibilidad de recuperar una contraseña o frase de paso en el entorno de Rescue and Recovery.
  - **Acceder al BIOS:** Abre el programa BIOS Setup Utility.
- **Comunicarse**
  - **Visión general sobre la comunicación:** Enlaza con los temas de ayuda relacionados en el entorno de Rescue and Recovery.
  - **Abrir navegador:** Iniciar el navegador Web Opera (el acceso a la Web o a la Intranet requiere una conexión Ethernet mediante cable).
  - **Descargar archivos**
  - **Correlacionar unidad de red:** Ayuda a los usuarios finales a acceder a las unidades de red para descargas de software o para la transferencia de archivos.
- **Resolver problemas**
  - **Visión general del diagnóstico:** Enlaza con los temas de ayuda de los diagnósticos de Rescue and Recovery.
  - **Diagnosticar hardware:** Abre la aplicación PC Doctor que puede realizar pruebas de hardware e informar de los resultados.
  - **Crear discos de diagnóstico**
  - **Arrancar desde otro dispositivo**
  - **Información del sistema:** Proporciona detalles acerca del sistema y de sus componentes de hardware.
  - **Registro de sucesos:** Proporciona detalles de las actividades recientes del usuario y listados del hardware del sistema para ayudar en la determinación y resolución de problemas. Un visor de registro proporciona una forma legible de visualizar las entradas del registro de activos y de actividad.
  - **Estado de la garantía**

Rescue and Recovery está disponible en sistemas PC de IBM y Lenovo que se proporcionen con el software preinstalado. También está disponible para su compra como un archivo descargable, de forma que las empresas puedan disfrutar también de las ventajas de Rescue and Recovery en sistemas que no sean de IBM ni de Lenovo.

El Apéndice B, “Parámetros y valores de TVT.TXT”, en la página 149 trata de la configuración del entorno de Rescue and Recovery para el despliegue. Aunque la instalación de Rescue and Recovery incluye la instalación de Rapid Restore Ultra, esta guía los trata como componentes individuales en las descripciones de personalización, configuración y despliegue.

Entorno de Windows de Rescue and Recovery

El entorno de Rapid Restore permite a los usuarios finales rescatar datos perdidos, aplicaciones y sistemas operativos con sólo pulsar un botón. Esta capacidad disminuye largas llamadas al Help Desk, lo que puede dar como resultado un ahorro en los costes del soporte.

Puede planificar las copias de seguridad de todos los sistemas de los usuarios finales , limitando con ello el riesgo y el tiempo de inactividad. Rescue and Recovery proporciona a los clientes un nivel adicional de soporte al realizar una configuración previa de la copia de seguridad externa automática en un servidor o en un dispositivo externo.

Antidote Delivery Manager

Antidote Delivery Manager es una infraestructura anti-virus y anti-gusanos incluida en ThinkVantage Rescue and Recovery. Los objetos son fáciles de implementar y eficaces, y permiten a un administrador inicializar el bloqueo y la recuperación en cuestión de minutos después de que se haya informado de un problema. Puede ser iniciada por un administrador y funciona en sistemas que no están conectados a la red. Antidote Delivery Manager complementa las herramientas antivirus existentes en lugar de sustituirlas, de forma que sigue siendo necesario mantener las herramientas de exploración de virus y de obtención de parches. Antidote Delivery Manager proporciona la infraestructura para detener la destrucción y aplicar los parches.

Cifrado de copias de seguridad

Las copias de seguridad se cifran por omisión con una clase de 256 AES. Si selecciona instalar Client Security Solution Versión 6.0, tiene la capacidad de cifrar utilizando Client Security Software Gina.

Client Security Solution 6.0

El propósito principal del software de Client Security Solution consiste en ayudar al cliente a proteger el PC como un activo, proteger los datos confidenciales que hay en el PC y proteger las conexiones de red a las que accede el PC. Para sistemas de IBM y de Lenovo que contienen el Módulo de plataforma fiable (TPM - Trusted Platform Module) compatible con Trusted Computing Group (TCG), el software de Client Security Solution (CSS) aprovechará el hardware como la raíz de confianza para el sistema. Si el sistema no contiene un chip de seguridad incorporado, Client Security Solution aprovechará las claves de cifrado basadas en software como la raíz de confianza del sistema. Las características de Client Security Solution 6.0 incluyen:

- **Autentificación segura de usuario**

  Requiere una frase de paso de Client Security protegida mediante hardware para los usuarios que acceden a las funciones protegidas de Client Security Solution.
- **Autentificación del usuario de huellas dactilares**

  Potencia la tecnología de huellas dactilares integrada y conectada mediante USB para autentificar a los usuarios en aplicaciones protegidas mediante contraseña.
- **Inicio de sesión de Windows basado en las huellas dactilares / frase de paso de Client Security**

  Requiere que los usuarios inicien sesión en Windows utilizando sus huellas dactilares o frase de paso de Client Security protegida mediante hardware.
- **Protección de datos**

Cifra los archivos importantes almacenándolos en una ubicación segura del disco duro que requiere autentificación válida de usuario y un chip de seguridad configurado correctamente.

- **Gestionar contraseñas de inicio de sesión**

  Gestionar y almacenar de forma segura información de inicio de sesión como por ejemplo los ID de usuario y las contraseñas.
- **Recuperación de la frase de paso/contraseña del usuario final**

  Permite a los usuarios recuperar por si solos una contraseña de Windows o una frase de paso de Client Security que hayan olvidado respondiendo preguntas configuradas previamente.
- **Auditar valores de seguridad**

  Permite a los usuarios ver una lista detallada de los valores de seguridad de la estación de trabajo y realizar los cambios para que satisfagan los estándares definidos.
- **Transferir certificados digitales**

  Protege mediante hardware la clave privada de los certificados de usuario y de la máquina.

Frase de paso de Client Security

La frase de paso de Client Security es una forma adicional opcional de autentificación de usuario que proporcionará seguridad mejorada a las aplicaciones de Client Security Solution. La frase de paso de Client Security tiene los requisitos siguientes:

- Debe tener como mínimo una longitud de ocho caracteres
- Debe contener como mínimo un dígito
- Debe ser diferente de las tres últimas frases de paso
- No debe contener más de dos caracteres repetitivos
- No debe empezar con un dígito
- No debe finalizar con un dígito
- No debe contener el ID de usuario
- No se debe cambiar si la frase de paso actual tiene menos de tres días de antigüedad
- No debe contener tres o más caracteres idénticos consecutivos a la frase de paso actual en cualquier posición
- No debe ser la misma que la contraseña de Windows.

La frase de paso de Client Security no es aceptable al mismo tipo de ataques que lo es la contraseña de Windows. Es importante tener en cuenta que el usuario individual también conoce una frase de paso de Client Security y que la única forma de recuperarse en caso de una frase de paso de Client Security olvidada es aprovechar la función de recuperación de contraseña de Client Security. Si el usuario ha olvidado las respuestas a sus preguntas de recuperación, no hay ninguna forma de recuperar los datos protegidos por la frase de paso de Client Security.

Recuperación de contraseña de Client Security

Este valor opcional permite a los usuarios registrados recuperar una contraseña de Windows o una frase de paso de Client Security olvidadas respondiendo correctamente a tres preguntas. Si esta característica está habilitada, durante el registro de Client Security del usuario final, cada usuario tendrá que seleccionar

tres respuestas a 10 preguntas seleccionadas previamente. Si el usuario olvida alguna vez su contraseña de Windows o su frase de paso de Client Security, tendrá la opción de responder a estas tres preguntas para restablecer su contraseña o frase de paso por sí mismo.

Notas:

1. Cuando se utiliza la frase de paso de Client Security, ésta es la única opción de recuperación de una frase de paso olvidado. Si el usuario olvida la respuesta a sus tres preguntas, el usuario estará obligado a volver a ejecutar el asistente de registro y perderá todos los datos anteriores protegidos mediante Client Security.
2. Cuando se utiliza Client Security para proteger el entorno del Área previa al escritorio de Rescue and Recovery, la opción Recuperación de contraseña visualizará de hecho la frase de paso de Client Security y/o la contraseña de Windows. Esto se debe a que el entorno del Área previa al escritorio no tiene la capacidad de realizar automáticamente un cambio de contraseña de Windows. Este comentario también es aplicable cuando un usuario de dominio que está colocado en la antememoria de forma local y no está conectado a la red realiza esta función en el inicio de sesión de Windows.

Software de huellas dactilares de ThinkVantage

El objetivo de las tecnologías de huellas dactilares biométricas de Lenovo es ayudar a los clientes a reducir los costes asociados con la gestión de contraseñas, mejorar la seguridad de sus sistemas y ayudar en el tratamiento del cumplimiento de las normas. Junto con los lectores de huellas dactilares, el Software de huellas dactilares de ThinkVantage le permite la autentificación de huellas dactilares en sus PC y en una red. La solución también se integra con Client Security Solution Versión 6.0 ofreciendo funcionalidad ampliada. Puede saber más sobre las tecnologías de huellas dactilares de Lenovo y descargar el software en la dirección:

www.thinkpad.com/fingerprint

El Software de huellas dactilares de ThinkVantage ofrece estas funciones:

- **Capacidades de software de cliente**
  - **Sustitución de la contraseña de Microsoft Windows**

    Sustitúyala con su huella dactilar para que un acceso al sistema sea fácil, rápido y seguro.
  - **Sustitución de la contraseña del BIOS (también denominada contraseña de encendido) y la contraseña de disco duro:** mediante las huellas dactilares para mejorar la comodidad y la seguridad del inicio de sesión.

    Sustituya estas contraseñas con su huella dactilar para mejorar la comodidad y la seguridad del inicio de sesión.
  - **Único acceso a Windows pasando el dedo:**

    Un usuario puede simplemente pasar el dedo UNA VEZ durante el arranque para obtener acceso al BIOS y a Windows, ahorrando un tiempo valioso.
  - **Integración con Client Security Solution** para utilizar con CSS Password Manager y para aprovechar el Módulo de plataforma segura (Trusted Platform Module). Los usuarios pueden pasar el dedo para acceder a sitios Web y seleccionar aplicaciones.
- **Características del administrador**
  - **Conmutar modalidades de seguridad:**

    Un administrador puede conmutar entre la modalidad segura y la modalidad cómo modificando los derechos de acceso de los usuarios con limitaciones.

- **Consola de gestión:**

  Ayuda a los administradores habilitando la personalización remota del software del Software de huellas dactilares mediante una interfaz de la línea de mandatos controlada por scripts.

- **Capacidades de seguridad**
  - **Seguridad del software:**

    Protege las plantillas de usuario mediante un fuerte cifrado cuando están almacenadas en un sistema y cuando se transfieren desde un lector al software.
  - **Seguridad del hardware:**

    Los lectores tienen un coprocesador de seguridad que almacena y protege las plantillas de huellas dactilares, las contraseñas del BIOS y las claves de cifrado.

Password Manager

Client Security Password Manager le permite gestionar y recordar toda la información importante y fácil de olvidar de inicio de sesión en los sitios Web y en las aplicaciones, como por ejemplo los ID de usuario, las contraseñas y otra información personal. Client Security Password Manager almacena toda la información mediante el chip de seguridad incorporado, de forma que el acceso a las aplicaciones y a los sitios Web permanece totalmente seguro.

Esto significa que en lugar de tener que recordar y proporcionar una gran cantidad de contraseñas individuales-- todas sujetas a diferentes normas y fechas de caducidad-- el usuario sólo tiene que recordar una única contraseña/frase de paso, proporcionar las huellas dactilares o una combinación de elementos de identificación.

Client Security Password Manager le permite realizar las funciones siguientes:

- **Cifra toda la información almacenada mediante el chip de seguridad incorporado**

  Client Security Password Manager cifra automáticamente toda la información mediante el chip de seguridad incorporado. Esto garantiza que toda la información importante de contraseñas está protegida mediante las claves de cifrado de Client Security Solution.

- **Transfiere de forma rápida y fácil los ID de usuario y las contraseñas utilizando una sencilla interfaz escribir-y-transferir**

  La interfaz escribir-y-transferir de Client Security Password le permite colocar la información directamente en la interfaz de inicio de sesión del navegador o de la aplicación. Esto ayuda a minimizar los errores de escritura y le permite guardar toda la información de forma segura mediante el chip de seguridad incorporado.

- **Escribe automáticamente los ID y contraseñas**

  Client Security Password Manager automatiza el proceso de inicio de sesión, entrando la información de inicio de sesión automáticamente al acceder a una aplicación o a un sitio Web cuya información de inicio de sesión se ha entrado en Client Security Password Manager.

- **Genera contraseñas aleatorias**

  Client Security Password Manager le permite generar contraseñas aleatorias para cada aplicación o sitio Web. Esto le permite aumentar la seguridad de los datos porque cada aplicación tendrá habilitada una protección de contraseña mucho más rigurosa. Las contraseñas aleatorias son mucho más seguras que las contraseñas definidas por el usuario porque la experiencia indica que la mayoría

de usuarios utilizan para las contraseñas información personal fácil de recordar y éstas son con frecuencia relativamente fáciles de averiguar.

- **Editar entradas utilizando la interfaz de Client Security Password Manager**

  Client Security Password Manager le permite editar todas las entradas de la cuenta y configurar todas las características opcionales de contraseña en una única interfaz fácil de utilizar. Esto hace más fácil y rápida la gestión de las contraseñas y de la información personal.

- **Acceda a la información de inicio de sesión desde la bandeja de iconos del escritorio de Microsoft(R) Windows(R) o mediante un simple atajo de teclado**

  El icono de Password Manager le otorga un fácil acceso a la información de inicio de sesión siempre que pueda necesitar añadir otra aplicación o sitio Web a Password Manager. También se puede acceder a todas las funciones de Client Security Password Manager mediante un simple atajo de teclado.

- **Exporte e importe información de inicio de sesión**

  Client Security Password Manager le permite exportar información importante de inicio de sesión de forma que puede llevarla de forma segura de un sistema a otro. Cuando exporta la información de inicio de sesión desde Client Security Password Manager, se crea un archivo de exportación protegido mediante contraseña que se puede almacenar en un soporte extraíble. Utilice este archivo para acceder a la información de usuario y a las contraseñas dondequiera que vaya, o importe las entradas en otro sistema mediante Password Manager.

  Nota: La importación sólo funcionará con Client Security Solution Versión 6.0. Client Security Software Versión 5.4X y las versiones anteriores no realizarán la importación en Client Security Solution 6.0 Password Manager.

SafeGuard PrivateDisk

Proteja los datos utilizando SafeGuard PrivateDisk. Cada todo el mundo almacena datos confidenciales en el PC. SafeGuard PrivateDisk protege los datos confidenciales. Funciona cómo una ″caja fuerte electrónica″ para la información confidencial y valiosa del sistema, todas las unidades de disco duro y los soportes extraíbles. Las personas que no estén autorizadas no podrán acceder a la información protegida ni leerla.

¿Cómo funciona SafeGuard PrivateDisk? SafeGuard PrivateDisk se basa en el principio de disco virtual.

- Se puede crear un disco virtual en cualquier unidad disponible
  - Soportes de memoria extraíbles (como por ejemplo, un disco, una llave USB, un CD-ROM, un DVD o una unidad Zip)
  - Discos duros, unidades de red
- El controlador funciona como una unidad de disco duro
  - El sistema operativo necesita grabar y leer mandatos en el controlador de forma transparente.
  - El controlador gestiona el almacenamiento cifrado.
  - Se cifran todos los datos y toda la información de directorios.
- SafeGuard PrivateDisk funciona con Client Security Solution y el Módulo de plataforma segura para proteger los certificados digitales generados por PrivateDisk
- SafeGuard PrivateDisk utiliza un algoritmo de cifras simétricas con una nueva clave AES aleatoria para cada disco virtual
  - AES, 128 bits, modalidad CBC

  - Nueva clave aleatoria para cada disco virtual
- Autentificación mediante:
  - Contraseña
  - Clave privada (certificado X.509), Smartcard opcional
  - Utilización de certificados EFS generados automáticamente si es posible
- Seguridad de contraseña:
  - PKCS#5
  - Retardo de tiempo después de una presentación de contraseña incorrecta
  - Diálogo de contraseña con ″protección de intercepción″

Security Advisor

La herramienta Security Advisor le permite visualiza un resumen de los valores de seguridad actualmente establecidos en el sistema. Puede revisar estos valores para visualizar el estado actual de la seguridad a fin de mejorar la seguridad del sistema. Algunos de los temas de seguridad que se incluyen son las contraseñas de hardware, las contraseñas de usuarios de Windows, la política de contraseñas de Windows, el protector de pantalla protegido y la compartición de archivos. Los valores por omisión de las categorías que se visualizan se pueden cambiar mediante el archivo TVT.txt.

Asistente de transferencia de certificados

El Asistente de transferencia de certificados de Client Security le guía por el proceso de transferir claves privadas asociadas con los certificados desde un proveedor de servicio de cifrado de Microsoft basado en software (CSP) al CSP de Client Security Solution basado en hardware. Después de la transferencia, las operaciones que utilizan los certificados serán más seguras porque las claves privadas estarán protegidas por el chip de seguridad incorporado.

Restablecimiento de la contraseña de hardware

Esta herramienta crea un entorno seguro que se ejecuta independientemente de Windows y le ayuda a restablecer contraseñas de la unidad de disco duro y de encendido olvidadas. La identidad se establece respondiendo a una serie de preguntas que el usuario crea. Es recomendable crear este entorno seguro lo antes posible, antes de que se olvide la contraseña. No podrá restablecer una contraseña de hardware olvidada hasta que se haya creado este entorno seguro en el disco duro y hasta después de que se haya registrado. Esta herramienta esta disponible sólo en sistemas ThinkCentre y ThinkPad.

Soporte de sistemas sin el Módulo de plataforma segura

Client Security Solution 6.0 ahora da soporte a sistemas de IBM y Lenovo que no tengan un chip de seguridad incorporado que cumpla las condiciones. Esto permitirá una instalación estándar en toda la empresa a fin de crear un entorno de seguridad homogéneo. Los sistemas que tienen el hardware del chip de seguridad incorporado serán fuertes contra ataques; sin embargo, las máquinas con sólo tengan el software también se beneficiarán de la seguridad y funcionalidad adicional.

System Migration Assistant

System Migration Assistant (SMA) es una herramienta de software que los administradores del sistema pueden utilizar para migrar un entorno de trabajo del usuario de un sistema a otro. El entorno de trabajo de un usuario incluye los elementos siguientes:

- Preferencias del sistema operativo, como por ejemplo los valores de conectividad de red y del escritorio
- Archivos y carpetas
- Valores personalizados de las aplicaciones, como por ejemplo los favoritos de un navegador Web o las preferencias de edición de Microsoft Word
- Cuentas de usuario

Los administradores del sistema pueden utilizar SMA para configurar un entorno de trabajo estándar para una empresa o para actualizar un sistema de un usuario individual. Los usuarios individuales pueden utilizar SMA para realizar una copia de seguridad del sistema o para migrar los valores y los archivos de un sistema a otro. Por ejemplo, desde un sistema de sobremesa a un sistema portátil.

Diferencias para OEM

Client Security Solution 6.0 no está disponible en este momento para sistemas OEM. Rescue and Recovery no aprovechará las aplicaciones de Client Security Solution en máquinas OEM.

Capítulo 2. Consideraciones sobre la instalación

Antes de instalar ThinkVantage Rescue and Recovery, debe comprender la arquitectura de toda la aplicación.

Rescue and Recovery

Rescue and Recovery tiene dos interfaces principales. La interfaz primaria funciona en el entorno Windows XP o Windows 2000. La interfaz secundaria (el entorno del Área previa al escritorio de Rescue and Recovery) funciona independientemente del sistema operativo Windows XP o Windows 2000, en el entorno PE de Windows.

Notas:

1. Rescue and Recovery sólo funcionará con una versión No de BIOS de Computrace si se ha instalado primero Rescue and Recovery y si Computrace está instalado. Consulte Capítulo 8, "Prácticas recomendadas", en la página 121
2. Si intenta instalar SMS en un sistema con Rescue and Recovery instalado con el área de Windows PE ya instalada en una partición virtual, SMS no se instalará. Tanto Windows PE como SMS utilizan el directorio C:\minint para su sistema de archivos. La forma de tener ambos instalados es instalar Rescue and Recovery 2.0 como una partición de tipo 12. Consulte "Instalación de Rescue and Recovery en una partición de servicio de tipo 12" en la página 135 para obtener instrucciones acerca de cómo instalar en el tipo 12.
3. Se puede crear un posible riesgo para la seguridad cuando Microsoft Recovery Console se instala en un sistema con Rescue and Recovery. Microsoft Recovery Console busca carpetas con la vía de acceso C:*\system32\config\ y si encuentra dicha vía de acceso asume que es un sistema operativo. Si las entradas del registro que requieren una contraseña de Windows no están presentes, la consola de recuperación permitirá al usuario seleccionar el sistema operativo y, a continuación, acceder a toda la unidad de disco duro sin necesidad de especificar ninguna contraseña.

Consideraciones sobre la sobreinstalación

Rescue and Recovery Versión 3.0 permite una operación de sobreinstalación de Rescue and Recovery 2.0.

Se recomienda que se realice una nueva copia de seguridad después de la instalación de Rescue and Recovery 3.0. Esto se puede realizar utilizando un script o la interfaz de usuario.

Existen pasos básicos que debe seguir para obtener un nuevo conjunto de copia de seguridad:

1. Copie las copias de seguridad anteriores en una unidad de CD/DVD o en una unidad de disco duro USB (si lo desea)
2. Suprima las copias de seguridad actuales
3. Realice una copia de seguridad base

El script siguiente copiará las copias de seguridad en una unidad de disco duro USB, suprimirá las copias de seguridad actuales y, a continuación, realizará una copia de seguridad base.

```
@echo off

::Cambie el directorio a \Archivos de programa\IBM\IBM Rescue and Recovery
cd %rr%

::copie las copias de seguridad en la unidad USB
rrcmd copy location=U

::Suprima todas las copias de seguridad de la unidad de disco duro local de forma
::silenciosa
rrcmd delete location=L level=0 silent

::Realice una nueva copia de seguridad base en la unidad de disco duro local de
::forma silenciosa
rrcmd backup location=L name="Rescue and Recovery 2.0 Base" silent
```

Client Security Solution

Cuando despliegue Client Security Solution 6.0, se deben tener en cuenta los aspectos siguientes.

Client Security Solution ha incluido en el código los controladores y el soporte de software necesario para habilitar el hardware de seguridad (Módulo de plataforma fiable) de la máquina que va a recibir Client Security Solution 6.0. La habilitación del hardware requiere como mínimo un arranque ya que el chip se controla realmente mediante el BIOS y requiere la autentificación satisfactoria en el BIOS a fin de que se complete el procedimiento. En otras palabras, si está establecida la contraseña de administrador/supervisor del BIOS, será necesario habilitar/inhabilitar el Módulo de plataforma fiable.

Antes de que el Módulo de plataforma fiable puede realizar ninguna función, se debe inicializar primero la “Propiedad”. Cada sistema tendrá sólo un administrador de Client Security Solution que controlará las opciones de Client Security Solution. Este administrador debe tener privilegios de administrador de Windows. El administrador se puede inicializar utilizando los scripts de despliegue XML.

Después de configurar la Propiedad del sistema, a cada usuario adicional de Windows que inicie sesión en el sistema el Asistente de configuración de Client Security le solicitará automáticamente que se registre e inicie las credenciales y las claves de seguridad del usuario.

Emulación de software para el Módulo de plataforma fiable

Client Security Solution tiene la opción de ejecutarse sin un Módulo de plataforma fiable en sistema cualificados. La funcionalidad será exactamente la misma exceptuando el hecho de que utilizará claves basadas en software en lugar de utilizar claves protegidas mediante hardware. El software también se puede instalar con un conmutador para forzarlo a utilizar siempre las claves basadas en software en lugar de aprovechar el Módulo de plataforma fiable. Esta decisión se toma en el momento de la instalación y no se puede invertir sin desinstalar y reinstalar el software.

Sintaxis para forzar una emulación de software del Módulo de plataforma fiable:

```
InstallFile.exe "/v EMULATIONMODE=1"
```

Escenarios de actualización

Consulte “Escenarios de software instalado” en la página 106 para obtener información acerca de cómo actualizar desde niveles anteriores de Client Security Solution.

Capítulo 3. Personalización de Rescue and Recovery

Este capítulo proporciona información que se puede utilizar para personalizar ThinkVantage Rescue and Recovery.

Producción de un Despliegue sencillo con el icono Crear copia de seguridad base del escritorio

Antes de iniciar este procedimiento, asegúrese de que los archivos TVT, como por ejemplo z062zaa1025us00.tvt, estén ubicados en el mismo directorio que el ejecutable o el archivo MSI; de lo contrario, la instalación fallará. Si el archivo se denomina setup_tvtrnr3_1027**c**.exe, ha descargado un paquete combinado. Estas instrucciones son para los archivos que se han descargado de forma separada de la página de descarga *Large Enterprise individual language files*.

Para realizar un despliegue simple que coloque para el usuario un icono de copia de seguridad en el escritorio, haga lo siguiente:

1. Extraiga SETUP_TVTRNR*XXXX*.EXE (donde *XXXX* es el ID de build) en un directorio temporal:

   ```
   start /WAIT setup.exe /a /s /v"/qn TARGETDIR="C:\TVTRR"" /w
   ```

2. Personalice el archivo TVT.TXT, según sea necesario. Por ejemplo, es posible que desee planificar una copia de seguridad semanal cada martes a las 3:00 p.m. Para conseguir esto, añada las entradas siguientes en la sección [Rescue and Recovery] de TVT.TXT. (Consulte el Apéndice B, "Parámetros y valores de TVT.TXT", en la página 149 para obtener información adicional de configuración.)

   ```
   ScheduleHour=15

   ScheduleMinute=00

   ScheduleDayOfTheWeek=2
   ```

3. Copie también Z062ZAA1025US00.TVT en C:\tvtrr. El archivo TVT debe estar en la misma carpeta que el archivo MSI.
4. Inicie la instalación MSI, aplazando el rearranque:

   ```
   start /WAIT msiexec /i "C:\TVTRR\Rescue and Recovery - client security
   solutions.msi" /qn REBOOT="R" /L*v %temp%\rrinstall.txt
   ```

   Nota: El mandato anterior se ha adecuado para que cupiera en esta página. Entre este mandato como una única cadena.
5. Personalice el entorno Rescue and Recovery. (Consulte "Área previa al escritorio" en la página 22 para obtener información detallada.)
6. Suprima los archivos temporales en el directorio C:\TVTRR. (Consulte "Entorno de Windows" en la página 18.)
7. Escriba un archivo de mandatos con los siguientes mandatos:

   ```
   del "c:\Documents and Settings\All Users\Desktop\Create Base Backup.lnk
   "%RR%rrcmd.exe" backup location=L name=Base level=0
   ```

   Nota: El mandato anterior se ha adecuado para que cupiera en esta página. Entre este mandato como una única cadena.
8. Cree un atajo de teclado en el escritorio de todos los usuarios denominado "Crear copia de seguridad base". (Especifique la vía de acceso debajo de **Escriba la ubicación** del elemento.)
9. Ejecute el programa de utilidad Sysprep en el sistema.
10. Cree la imagen para el despliegue.

Después de que el usuario cliente recibe la imagen y personaliza el sistema, el usuario pulsa el icono **Crear copia de seguridad base** para iniciar Rescue and Recovery y guarda la copia de seguridad base.

Captura de una imagen Sysprep en la copia de seguridad base

Para capturar una imagen del programa de utilidad Sysprep en la copia de seguridad base, haga los siguiente:

1. Realice una instalación administrativa:

```
:: Extraiga el archivo WWW EXE en el directorio C:\IBMRR
     start /WAIT setup_tvtrnrXXXX.exe /a /s /v"/qn TARGETDIR="C:\TVTRR"" /w
```

2. Añada la siguiente sección al final del archivo TVT.TXT en C:\TVTRR\Archivos de programa\IBM ThinkVantage\Rescue and Recovery

```
[Backup0]
BackupVersion=2.0
```

3. Instale Rescue and Recovery utilizando el archivo MSIEXE:
   a. Para todos los MSI, añada el siguiente código de generación del registro de instalación:

```
/L*v %temp%\rrinstall.txt
```

   b. Para instalar los archivos de instalación utilizando el archivo MSIEXE, especifique el siguiente mandato:

```
: Realice la instalación de Rescue and Recovery

 msiexec /i "C:\TVTRR\Rescue and Recovery - Client
Security Solution.msi"
```

   c. Para instalar de forma silenciosa los archivos de instalación utilizando MSIEXE:

      Rearrancando al final, especifique el siguiente mandato:

```
: Instalación silenciosa utilizando MSI con un rearranque
: Escriba el siguiente mandato en una línea

start /WAIT msiexec /i "C:\TVTRR\Rescue and Recovery - Client
Security Solution.msi" /qn
```

      Suprimiendo el rearranque, especifique el mandato siguiente:

```
: Instalación silenciosa utilizando el MSI sin un rearranque
: Escriba el siguiente mandato en una línea

start /WAIT msiexec /i "C:\TVTRR\Rescue and Recovery - Client
Security Solution.msi" /qn REBOOT="R"
```

4. Especifique los mandatos siguientes:

```
:Inicie el servicio de Rescue and Recovery
net start  "TVT Backup Service"

:Cree la Copia de seguridad base Sysprep en la unidad de disco duro local
: Escriba el siguiente mandato en una sola línea

cd \"Archivos de programa"\"IBM ThinkVantage\Rescue and Recovery"
rrcmd sysprepbackup location=l name=Copia de seguridad Sysprep"
```

   Si desea utilizar una contraseña, añada la sintaxis `password=`*`pass`*.
5. Ejecute la implementación específica de Sysprep cuando vea el siguiente mensaje:

```
************************************************
** Ready to take sysprep backup.               **
** PLEASE RUN SYSPREP NOW AND SHUT DOWN.       **
**                                             **
** Next time the machine boots, it will boot   **
** to the PreDesktop Area and take a backup.   **
************************************************
```

6. Cuando finalice Sysprep, concluya el sistema y rearranque la máquina.

   Nota: El sistema operativo arrancará en el Area previa al escritorio de Rescue and Recovery. Verá una barra de estado que indica **Restauración del sistema en progreso**
7. Cuando se complete, verá un mensaje que indica **La copia de seguridad de Sysprep ha finalizado**.
8. Apague el sistema utilizando el botón de encendido.
9. Capture la imagen para el despliegue.

Captura de una máquina con varias particiones y exclusión de archivos en una copia de seguridad de Sysprep

Para capturar varias particiones en una copia de seguridad del programa de utilidad Sysprep, haga lo siguiente:

1. Realice una instalación administrativa:

   ```
   :: Extraiga WWW EXE al directorio C:\TVTRR
        start /WAIT setup_tvtrrXXXX.exe /a /s /v"/qn TARGETDIR="C:\TVTRR"" /w
   ```

2. Asegúrese o añada la siguiente sección al final del archivo TVT.TXT de C:\\"Archivos de programa"\"IBM ThinkVantage\Rescue and Recovery":\tvtrr\

   ```
   [Backup0]
   BackupVersion=2.0

   [BackupDisk]
   CustomPartitions=0
   ```

   Para EXCLUIR una partición, añada lo siguiente al archivo TVT.TXT:

   ```
   [BackupDisk]
   CustomPartitions=1

   [PartitionX].
   IncludeInBackup=0
   ```

   donde **X** es el número de la partición
3. Si desea excluir los archivos .MPG y JPG de las copias de seguridad, añádalos a IBMFILTER.TXT como en el ejemplo siguiente:

   ```
   X=*.JPG
   X=*.MPG
   ```

4. Instale Rescue and Recovery utilizando MSIEXE:
   a. Para todos los MSI, añada el siguiente código de generación de registro de instalación:

      ```
      /L*v %temp%\rrinstall.txt
      ```

   b. Para instalar los archivos de instalación utilizando MSIEXE, especifique el mandato siguiente:

      ```
      : Realice la instalación de Rescue and Recovery

       msiexec /i "C:\TVTRR\Rescue and Recovery - Client Security Solutiion.msi"
      ```

c. Para instalar de forma silenciosa los archivos de instalación utilizando MSIEXE:

   Especifique el siguiente mandato y rearranque cuando finalice:

   ```
   : Instalación silenciosa utilizando el MSI con un rearranque

   : Especifique el siguiente mandato en una única línea
   start /WAIT msiexec /i "C:\TVTRR\Rescue and Recovery - Client
   Security Solutiion.msi" /qn
   ```

   Sin el rearranque, especifique el siguiente mandato:

   ```
   : Instalación silenciosa utilizando el MSI sin un rearranque

   : Especifique el siguiente mandato en una única línea
   start /WAIT msiexec /i "C:\TVTRR\Rescue and Recovery -
   Client Security Solutiion.msi" /qn REBOOT="R"
   ```

5. Especifique los mandatos siguientes:

   ```
   :Inicie el servicio de Rescue and Recovery
   net start  "TVT Backup Service"

   :Cree una copia de seguridad de Sysprep en la unidad de disco duro local

   : Especifique el siguiente mandato en una única línea
   cd \"Archivos de programa"\IBM ThinkVantage Rescue and Recovery"
   rrcmd sysprepbackup location=L name="Sysprep Base Backup"
   ```

   Si desea utilizar una contraseña, añada la sintaxis `password=`*`pass`*.

6. Ejecute la implementación específica de Sysprep cuando vea el siguiente mensaje:

   ```
   ************************************************
   ** Ready to take sysprep backup.               **
   ** PLEASE RUN SYSPREP NOW AND SHUT DOWN.       **
   **                                             **
   ** Next time the machine boots, it will boot   **
   ** to the PreDesktop Area and take a backup.   **
   ************************************************
   ```

7. Cuando finalice Sysprep, concluya el sistema y rearranque la máquina.

   Nota: El sistema operativo arrancará en el Area previa al escritorio de Rescue and Recovery. Verá una barra de estado que indica **Restauración del sistema en progreso**

8. Cuando se complete, verá un mensaje que indica **La copia de seguridad de Sysprep ha finalizado**.
9. Apague el sistema utilizando el botón de encendido.
10. Capture la imagen para el despliegue.

Entorno de Windows

Inclusión y exclusión de archivos en las copias de seguridad

Rescue and Recovery tiene amplias funciones de inclusión y exclusión. Puede incluir y excluir un archivo individual, carpeta o toda una partición.

Los archivos que controlan las funciones de inclusión y exclusión, listados en orden de precedencia, son los siguientes. Todos los archivos están ubicados en el directorio C:\Archivos de programa\ibm thinkvantage\rescue and recovery.

1. IBMFILTER.TXT
2. GUIEXCLD.TXT

El usuario final, por omisión, puede seleccionar archivos y carpetas individuales para que se excluyan de la copia de seguridad. Estos archivos y carpetas se almacenan en el archivo GUIEXCLD.TXT.

Si un administrador desea asegurarse de que siempre se realiza copia de seguridad de un archivo o carpeta determinados, el administrador puede incluir los nombres o tipos de archivo en el archivo IBMIFILTER.TXT. Todas las entradas en este archivo se incluirán siempre en una copia de seguridad, independientemente de las entradas en el archivo GUIEXCLD.TXT.

Los administradores también pueden excluir siempre un archivo, carpeta o partición de una copia de seguridad.

Los siguientes archivos se excluirán siempre de cualquier copia de seguridad:
- PAGEFILE.SYS
- HIBERFILE.SYS
- C:\SYSTEM VOLUME INFORMATION

Cuando se realice la restauración, Windows volverá a generar automáticamente tanto PAGEFILE.SYS como HIBERFILE.SYS. Además, una vez que se haya restaurado la copia de seguridad, Windows volverá a generar los datos de Restauración del sistema de Windows con un nuevo punto de restauración.

IBMFILTER.TXT

El formato del archivo es el siguiente:

- Una línea por cada entrada de norma de inclusión/exclusión.
- Si se aplica más de una norma a un archivo o carpeta, se aplicará la última norma. Las entradas de la parte inferior del archivo tienen prioridad.
- Las entradas deben empezar con una de las opciones siguientes:
  - **;**

    para un comentario
  - **I**

    debe incluir archivos o carpetas que coincidan con la entrada
  - **X**

    debe excluir archivos o carpetas que coincidan con la entrada
  - **S**

    debe incluir Almacenamiento de instancia única en un archivo o una carpeta
  - **i**

    para archivos o carpetas que seleccione incluir
  - **x**

    para archivos o carpetas que seleccione excluir
  - **s**

    se utiliza opcionalmente para identificar un archivo o carpeta como Almacenamiento de instancia única que se incluiría normalmente.

```
  S=*
  X=*
  i=*
I=*.ocx
I=*.dll
I=*.exe
I=*.ini
I=*.drv
I=*.com
I=*.sys
I=*.cpl
I=*.icm
I=*.lnk
I=*.hlp
I=*.cat
I=*.xml
I=*.jre
I=*.cab
I=*.sdb
I=*.bat
I=?:\ntldr
I=?:\peldr
I=?:\bootlog.prv
I=?:\bootlog.txt
I=?:\bootsect.dos
I=?:\WINNT\*
I=?:\WINDOWS\*
X=?:\WINDOWS\prefetch\*
I=?:\minint\*
I=?:\preboot\*
I=?:\Application Data\*
I=?:\Documents and Settings\*
I=?:\IBMTOOLS\*
I=?:\Archivos de programa\*
I=?:\msapps\*
  X=?:\Recycled
  X=?:\RECYCLER
  x=?:\Documents and Settings\*\Cookies\*
x=?:\Documents and Settings\*\Local Settings\History\*
X=?:\Documents and Settings\*\Local Settings\Temp\*
x=?:\Documents and Settings\*\Local Settings\Temporary Internet Files\*
x=?:\Documents and Settings\*\Desktop\*
x=?:\Documents and Settings\*\My Documents\*
  s=?:\Documents and Settings\*\Desktop\*
  s=?:\Documents and Settings\*\My Documents\*
  x=*.vol
  s=*.vol
```

Personalización de otros aspectos de Rescue and Recovery

Puede personalizar muchos aspectos de Rescue and Recovery utilizando un archivo externo denominado TVT.TXT que se define antes del proceso de instalación. El archivo TVT.TXT está ubicado en el subdirectorio C:\Archivos de programa\IBM ThinkVantage\.

El archivo TVT.TXT seguirá el formato estándar del archivo INI de Windows con los datos organizados por secciones indicadas por [] y una entrada por línea con este formato:

```
setting=valor
```

Por ejemplo, si no desea cifrar todos los datos de copia de seguridad, incluya las líneas siguientes en el archivo TVT.TXT:

```
[Rescue and Recovery]
EncryptBackupData=0
```

El parámetro `0` a continuación de EncryptBackupData indica a Rescue and Recovery que no cifre la copia de seguridad.

En el Apéndice B, "Parámetros y valores de TVT.TXT", en la página 149 se presenta una lista completa de las series de valores, parámetros y valores por omisión para la sección [Rescue and Recovery] del archivo TVT.TXT.

Informe de problema

Actualmente, no existe ninguna forma de transmitir automáticamente mediante FTP o correo electrónico desde el entorno de Rescue and Recovery; se indicará al usuario final que utilice el correo electrónica integrado en el navegador así como la ubicación de los archivos que se deben transmitir. No se da soporte a la transferencia dinámica de datos, pero la función de registro se empaquetará con los sucesos de registro en un archivo y se indicará al usuario la ubicación del paquete y el nombre del archivo que se pueden enviar por correo electrónico. Esto creará el archivo XML *Req 115 Trouble Ticket*, que combina toda la información que se visualiza en la Información del sistema (Current HW, eGatherer e información de registro de diagnóstico de PCDR), que se colocará en una ubicación que se pueda encontrar fácilmente y que sea accesible tanto desde el entorno de Rescue and Recovery como desde el SO – C:\IBMSHARE.

Diagnósticos: es una aplicación base disponible en el Área previa al escritorio que ayuda en la determinación de problemas. La salida de estas pruebas se almacenará de forma que pueda ser visualizada por un Help Desk o transmitida al mismo. Rescue and Recovery proporcionará herramientas para realizar la recuperación de una versión del entorno de Windows del usuario de la que se ha realizado una copia de seguridad anteriormente.

Rescue and Recovery contendrá herramientas para realizar una completa restauración de una partición de usuario a una versión anterior así como herramientas para recuperar archivos individuales. Las herramientas proporcionarán acceso a una copia de seguridad de los datos del usuario. Estas herramientas proporcionarán la capacidad de recuperar todos estos datos, o algunos de ellos.

OSFILTER.TXT

Este archivo recupera el sistema operativo y las aplicaciones del usuario sin afectar los datos de los mismos. Rescue and Recovery proporciona la capacidad de restaurar de forma selectiva archivos y carpetas individuales (incluyendo subcarpetas) utilizando numeración explícita y filtrado mediante caracteres comodín sin borrar otros datos. Un archivo externo definirá los archivos, carpetas o tipos de archivos (aprovechando los caracteres comodín) que forman parte del sistema operativo y de las aplicaciones. El administrador puede personalizar este archivo y se proporcionará un archivo externo por omisión. Cuando el usuario selecciona recuperar el sistema operativo, verá un menú que le permite seleccionar Restaurar solamente con las siguientes opciones de Windows: Solamente se restaurarán los archivos que coincidan con las normas contenidas en este archivo externo. El administrador puede personalizar el contenido de este archivo externo.

Para visualizar el archivo OSFILTER.TXT, utilice esta vía de acceso: `cd %RR%`. Consulte "IBMFILTER.TXT" en la página 19 para obtener información sobre el formato de archivo.

Área previa al escritorio

Para personalizar partes del Área previa al escritorio de Rescue and Recovery, que se inicia incluso si el sistema operativo no se abre, utilice el programa de utilidad RRUTIL.exe para obtener (GET) and poner (PUT) archivos. Estos archivos y sus opciones de personalización se listan en la tabla siguiente:

Tabla 1. Archivos RRUTIL.exe y opciones de personalización

Archivo / Directorio	Opciones de personalización
\MININT\SYSTEM32 WINBOM.INI	Añade una dirección IP estática, cambia la resolución de vídeo
\MININT\INF \MININT\SYSTEM32\DRIVERS	Añade controladores de dispositivo
MAINBK.BMP	Modifica el fondo del entorno
MINIMAL_TOOLBAR(1).INI	Inhabilita la barra de direcciones
NORM1.INI	Configura el navegador Opera, inhabilita la barra de direcciones de Opera, cambia los valores del proxy de Opera, especifica un directorio de descarga fijo, añade una extensión de archivo específica a la lista de archivos descargables, cambia el comportamiento de los archivos con extensiones específicas
OPERA_010.CMD	Excluye los favoritos de los usuarios de Windows
OPERA6.INI	Configura el navegador Opera, inhabilita la barra de direcciones
PEACCESS*xx*.INI (donde *xx* s la indicación del idioma)	Entorno previo al arranque: fonts de la GUI principal, fondo del entorno, entradas y funciones de los paneles derecho e izquierdo, sistema de ayuda basado en HTML
STANDARD_MENU.INI	Habilita la visualización de la ventana ″Guardar como″

Utilización de RRUTIL.EXE

Puede obtener RRUTIL.EXE y otros programas de utilidad mencionados en esta guía en el sitio Web que contiene este documento.

El procedimiento siguiente lista los pasos para obtener (GET) archivos de, y poner (PUT) archivos en, el entorno de Rescue and Recovery. Estos procedimientos se utilizan para todas las personalizaciones de archivos del entorno de Rescue and Recovery.

Para utilizar RRUTIL.EXE, haga lo siguiente:

1. Copie RRUTIL.exe en la raíz de la unidad C.
2. Cree un archivo GETLIST.TXT con la sintaxis siguiente:

   ```
   \preboot\usrintfc\nombre archivo
   ```

   Guarde el archivo como C:\TEMP\GETLIST.TXT.
3. En el indicador de la línea de mandatos, escriba el mandato RRUTIL.exe y uno de los conmutadores definidos en la tabla siguiente. A continuación, complete el mandato con los parámetros adecuados, tal como se muestra en la tabla siguiente.

Tabla 2. Mandato y opciones de conmutación

Mandato y opciones de conmutación	Resultado
`RRUTIL -l1`	Lista el contenido del directorio preboot
`RRUTIL -l2`	Lista el contenido del directorio minint
`RRUTIL -l4`	Lista el contenido de la raíz de la unidad C o de la raíz de la partición de tipo 12
`RRUTIL -g C:\temp\getlist.txt C:\temp`	Obtiene archivos de la partición preboot
`RRUTIL -d C:\temp\ dellist.txt`	Suprime archivos de la partición preboot.
`RRUTIL -p C:\temp`	Añade o sustituye archivos de la partición preboot.
`RRUTIL -r` *`vía_acceso \nombre_antiguo.ext nombre_nuevo.ext`* `RRUTIL -r \temp\rr\test.txt test2.txt` el archivo está en el directorio preboot\rr	Renombra un archivo del Área previa al escritorio.
`RRUTIL -bp C:\temp`	Actualiza o sustituye archivos de la partición virtual RRBACKUPS.
`RRUTIL -bl` *`vía_acceso`* RRUTIL -bl lista en `C:\rr-list.txt` `rrutil -bl c:\rrtemp`	Lista el directorio RRBACKUPS
`RRUTIL -br RRbackups\C\n` donde n es el número de copia de seguridad	Suprime el contenido de la copia de seguridad.
`RRUTIL -bg C:\temp\bgetlist.txt C:\temp`	Copia archivos individuales de \RRBACKUPS.
`RRUTIL -s`	Espacio utilizado por RRBACKUPS.

4. Después de haber realizado la rutina GET, puede editar el archivo utilizando un editor de texto estándar.

Ejemplo: PEACCESSIBMxx.INI

Este ejemplo hace referencia a PEACCESSIBM*xx*.INI, que es un archivo de configuración donde puede personalizar elementos del entorno de Rescue and Recovery (consulte “Personalización del entorno previo al arranque” en la página 25).

Nota: *xx* en el nombre del archivo representa una de las siguientes abreviaturas de idioma de dos letras:

Tabla 3. Códigos de idioma

Código de idioma de dos letras	Idioma
br	Portugués de Brasil
dk	Danés
en	Inglés
fi	Finlandés
fr	Francés
gr	Alemán
it	Italiano
jp	Japonés
kr	Coreano
nl	Holandés
no	Noruego
po	Portugués
sc	Chino simplificado
sp	Español
sv	Sueco
tc	Chino tradicional

Obtención del archivo PEACCESSIBMEN.INI del entorno de Rescue and Recovery:

1. Cree el archivo GETLIST.TXT con los parámetros siguientes:

   ```
   \preboot\reboot\usrintfc\PEAccessIBMen.ini
   ```
2. Guarde el archivo como C:\TEMP\GETLIST.TXT.
3. En el indicador de la línea de mandatos, especifique el mandato siguiente:

   ```
   C:\RRUTIL-g C:\temp\getlist.txt C:\temp
   ```

Colocación del archivo PEACCESSIBMEN.INI de nuevo en el entorno de Rescue and Recovery. En la línea de mandatos, emita el siguiente mandato:

```
C:\RRUTIL.EXE -p C:\temp
```

Nota: La rutina PUT (**-p**) utiliza la estructura de directorios creada en la rutina GET (**-g**). Para una colocación correcta del archivo editado, asegúrese de que el archivo editado se coloca en el mismo directorio que está establecido en el archivo GETLIST.TXT, como en el ejemplo siguiente:

```
C:\temp\preboot\usrintfc\PEAccessIBMen.ini
```

Ejemplo: Adición de controladores de dispositivos al Área previa al escritorio

1. Obtenga los controladores de dispositivo del sitio Web del proveedor o de otro medio.
2. Cree las siguientes estructuras de directorios:

   ```
   C:\TEMP\MININT\INF
   ```

   ```
   C:\TEMP\MININT\SYSTEM32\DRIVERS
   ```
3. Copie todos los archivos *.INF del controlador de red en el directorio MININT\INF. (Por ejemplo, es necesario que E100B325.INF esté en el directorio \MININT\INF.)
4. Copie todos los archivos *.SYS en el directorio \MININT\SYSTEM32\DRIVERS. (Por ejemplo, es necesario que E100B325.SYS esté en el directorio MININT\SYSTEM32\DRIVERS.)
5. Copie los archivos relacionados *.DLL, *.EXE u otros en el directorio \MININT\SYSTEM32\DRIVERS. (Por ejemplo, los archivos E100B325.DIN o INTELNIC.DLL deben estar en el directorio MININT\SYSTEM32\DRIVERS.)

Notas:

a. Los archivos de catálogo no son necesarios, ya que no se procesan en el entorno de Rescue and Recovery. Las instrucciones anteriores se aplican a cualquier controlador de dispositivo que pueda ser necesario para configurar el sistema.
b. Debido a la limitación de Windows Professional Edition, es posible que tenga que aplicar manualmente algunas aplicaciones o algunos valores de configuración como actualizaciones del registro.

6. Para poner los controladores de dispositivo en el entorno de Rescue and Recovery, especifique lo siguiente en la línea de mandatos:

```
C:\ RRUTIL.EXE -p C:\temp
```

Personalización del entorno previo al arranque

Si edita el archivo de configuración PEACCESSIBM*xx*.INI (donde *xx* es la indicación de idioma), puede personalizar los elementos siguientes del entorno de Rescue and Recovery:

- Los fonts principales de la GUI
- El fondo del entorno
- Las entradas y funciones del panel izquierdo de la interfaz de usuario
- El sistema de ayuda basado en HTML para el entorno de Rescue and Recovery

Nota: Para obtener, editar y sustituir el archivo PEACCESSIBMEN.INI, consulte el "Ejemplo: PEACCESSIBMxx.INI" en la página 23.

Modificación del font de la GUI principal

Puede modificar el font de la interfaz principal gráfica de usuario (GUI). Es posible que los valores por omisión no visualicen todos los caracteres correctamente, dependiendo del idioma y de los caracteres necesarios. En PEACCESSIBM*xx*.INI (where *xx* es la indicación de idioma), la sección [Fonts] contiene los valores por omisión para el estilo de carácter que se visualiza. Los siguientes son los valores por omisión para la mayoría de idiomas con un conjunto de caracteres de un solo byte:

```
[Fonts]
LeftNavNorm = "Microsoft Sans Serif"
LeftNavBold = "Arial Bold"
MenuBar = "Microsoft Sans Serif"
```

En función de los requisitos del conjunto de caracteres y de visualización, los siguientes fonts son compatibles con el entorno de Rescue and Recovery. Es posible que otros fonts sean compatibles, pero no se han probado:

- Courier
- Times New Roman
- Comic Sans MS

Modificación del fondo del entorno

El fondo del panel derecho es un mapa de bits, MAINBK.BMP, que está ubicado en el directorio \PREBOOT\USRINTFC. Si crea su propia imagen de mapa de bits para el fondo del panel derecho, debe adecuarse a las siguientes dimensiones:

- 620 píxeles de ancho
- 506 píxeles de profundidad

Debe colocar el archivo en el directorio \PREBOOT\USRINTFC para que Rescue and Recovery presente el fondo que desea.

Nota: Para obtener, editar y sustituir el archivo MAINBK.BMP, consulte el "Utilización de RRUTIL.EXE" en la página 22.

Modificación de las entradas y funciones del panel izquierdo

La modificación de las entradas del panel izquierdo requiere la edición del archivo PEACCESSIBM*xx*.INI (donde *xx* es la indicación de idioma). Para obtener información acerca de cómo obtener PEACCESSIBM*xx*.INI desde el entorno de Rescue and Recovery y acerca de cómo sustituir el archivo, consulte "Utilización de RRUTIL.EXE" en la página 22.

Rescue and Recovery tiene veintiuna entradas en el panel izquierdo. Aunque las funciones son distintas, cada entrada tiene los mismos elementos básicos. El siguiente es un ejemplo de una entrada del panel izquierdo:

```
[LeftMenu] button00=2, "Introduction", Introduction.bmp, 1,
1, 0, %sysdrive%\Preboot\Opera\ENum3.exe,
```

Tabla 4. Entradas del panel izquierdo y opciones de personalización

Entrada	Opciones de personalización
00-01	Completamente personalizable.
02	Debe permanecer un botón de tipo 1 (consulte la Tabla 5). El texto se puede cambiar. Se puede definir una aplicación o función de ayuda. No se puede añadir ningún icono.
03-06	Completamente personalizable.
07	Debe permanecer un tipo 1. El texto se puede cambiar. Se puede definir una aplicación o función de ayuda. No se puede añadir ningún icono.
08-10	Completamente personalizable.
11	Debe permanecer un botón de tipo 1. El texto se puede cambiar. Se puede definir una aplicación o función de ayuda. No se puede añadir ningún icono.
16	Debe permanecer un tipo 1. El texto se puede cambiar. Se puede definir una aplicación o función de ayuda. No se puede añadir ningún icono.
17–22	Completamente personalizable.

Definición de tipos de entrada: **`Button00`** debe ser un identificador exclusivo. El número determina el orden en el que los botones se visualizan en el panel izquierdo.

`Button00=[0-8]` Este parámetro determina el tipo de botón. Este número puede ser un entero de 0 a 8. La tabla siguiente explica el tipo y comportamiento de cada tipo de botón:

Tabla 5. Parámetros del tipo de entrada

Parámetro	Tipo de botón
`0`	Campo vacío. Utilice este valor cuando desee dejar una fila en blanco y sin utilizar.
`1`	Texto de cabecera de la sección. Utilice este valor para establecer una cabecera principal de grupo o sección.
`2`	Inicio de la aplicación. Define un archivo de mandatos o aplicación para que se inicie cuando el usuario pulse el botón o texto.

Tabla 5. Parámetros del tipo de entrada (continuación)

Parámetro	Tipo de botón
3	Ayuda de Opera para el entorno de Rescue and Recovery. Define un tema de ayuda para que se inicie utilizando el navegador Opera
4	Visualiza una ventana de mensaje de reinicio antes del inicio. Utiliza estos valores para indicar a la GUI que presente un mensaje al usuario indicando que se debe reiniciar el sistema antes de que se ejecute la función especificada.
5	Reservado para Lenovo Group Ltd
6	Reservado para Lenovo Group Ltd
7	Inicia y espera. Los campos que van a continuación de esta especificación fuerzan al entorno a esperar un código de retorno de la aplicación iniciada antes de continuar. Se espera que el código de retorno esté en la variable de entorno, %errorlevel%.
8	Inicia la aplicación. La GUI recupera el Código de país y el idioma antes de iniciar la aplicación. Se utiliza para enlaces Web que tienen scripts CGI para abrir una página Web desde un país determinado o en un idioma específico.
9	Reservado para Lenovo Group Ltd
10	Reservado para Lenovo Group Ltd

Definición de campos vacíos:

Button00=[0-10], "título"
El texto a continuación del parámetro del tipo de botón especifica el texto o título del botón. Si el texto sobrepasa la anchura del panel izquierdo, el texto se cortará y unos puntos suspensivos indicarán que siguen más caracteres. El texto completo del título se visualiza al utilizar la ayuda flotante.

Button00=[0-10], "título", file.bmp
A continuación del texto del título, especifique el nombre del archivo del mapa de bits que desea utilizar como icono para el botón que se está creando. Para que quepa correctamente, el mapa de bits no debe ser más grande de 15 píxeles por 15 píxeles.

Button00=[0-10], "título", archivo.bmp, [0 o 1]
Este valor indica al entorno que visualice u oculte la entrada. El valor 0 oculta la entrada. Si se establece el valor en 0, se visualizará una línea en blanco. El valor 1 visualiza el valor.

Button00=[0-10], "título", archivo.bmp, [0 o 1], 1
Es una función reservada y se debe establecer siempre en 1.

Button00=[0-10], "title", archivo.bmp, [0 o 1], 1, [0 o 1]
Para necesitar una contraseña antes de iniciar una aplicación, coloque un valor de 1 en esta posición. Si establece este valor en 0, no será necesaria ninguna contraseña antes de que se haya iniciado una aplicación especificada.

Button00=[0-10], "título", archivo.bmp, [0 o 1], 1, [0 o 1], %sysdrive%[pathname\executable]
El valor de %sysdrive@ debe ser la letra de la unidad de arranque. A

continuación de la letra de la unidad de arranque, debe proporcionar una vía de acceso calificada totalmente de un archivo de mandatos o aplicación.

Button00=[0-10], "título", archivo.bmp, [0 o 1], 1, [0 o 1],%sysdrive%[pathname\executable], [parameters]
Proporciona cualquier número de parámetros necesario por la aplicación de destino que se está iniciando.

Si no proporciona valores para varios campos, debe proporcionar las comas necesarias a fin de que se acepte la definición del botón y de que se ejecute correctamente. Por ejemplo, si está creando una cabecera de grupo, ″Rescue and Recover″, el código para la entrada sería:

```
Button04=1, "Rescue and Recover",,,,,,
```

Las entradas 02, 07, 11 y 16 deben permanecer entradas del tipo `0` (o cabecera) y siempre se deben encontrar en sus espacios numéricos. La disponibilidad de entradas que se encuentran debajo de las cabeceras se puede reducir estableciendo entradas totalmente personalizables en líneas en blanco de tipo 0 en el panel izquierdo. Sin embargo, el número total de entradas no puede exceder de veintitrés.

La tabla siguiente muestra la función y los ejecutables que puede iniciar desde las entradas del panel izquierdo:

Tabla 6. Funciones y ejecutables del panel izquierdo

Función	Ejecutable
Recuperar archivos	WIZRR.EXE
Restaurar a partir de la copia de seguridad	WIZRR.EXE
Crear un archivo de migración	WIZRR.EXE
Abrir navegador	OPERA.EXE
Correlacionar una unidad de red	MAPDRV.EXE
Diagnosticar hardware	RDIAGS.CMD; inicia la aplicación PC Dr, sólo en modelos con preinstalación de IBM y Lenovo
Crear disquetes de diagnósticos	DDIAGS.CMD

Modificación de las entradas y funciones del panel derecho

La modificación de las entradas del panel derecho requiere la edición del archivo PEACCESSIBM*xx*.INI (donde *xx* es la indicación de idioma). Para obtener información acerca de cómo obtener PEACCESSIBM*xx*.INI desde el entorno de Rescue and Recovery y acerca de cómo sustituir el archivo, consulte “Ejemplo: PEACCESSIBMxx.INI” en la página 23.

Los enlaces a las funciones, los mensajes de usuario y el estado de la ventana del panel derecho son personalizables.

Personalización de los enlaces de las funciones del panel derecho: Para cambiar las funciones de los enlaces que se entienden en la parte superior del panel derecho, modifique la sección [TitleBar] de PEACCESSIBM*xx*.INI (donde *xx* es la indicación de idioma). Estos enlaces funcionan de la misma manera que las entradas del panel izquierdo. Los valores del número de botón van del 00 al 04. Las mismas aplicaciones que se pueden iniciar desde el panel izquierdo se pueden

iniciar desde las entradas de [TitleBar]. Consulte “Utilización de RRUTIL.EXE” en la página 22 para ver una lista completa de ejecutables que se pueden iniciar desde la barra del título.

Modificación de los mensajes de usuario y del estado de la ventana: PEACCESSIBM*xx*.INI (donde *xx* es la indicación de idioma) contiene dos secciones con mensajes para el usuario que se pueden modificar:

```
[Welcome window]
[Reboot messages]
```

La ventana de bienvenida está definida en la sección [Welcome] de PEACCESSIBM*xx*.INI (donde *xx* es la designación de idioma). En función de los cambios que haya realizado en el panel izquierdo, puede cambiar la información en la línea del título y las líneas de la 01 a la 12. Puede establecer el font en el que se visualizarán el título, la cabecera y negrita:

```
[Welcome]
Title = "Bienvenido a Rescue and Recovery"
Line01 = "El espacio de trabajo de Rescue and Recovery(TM) proporciona una serie
de herramientas para ayudarle a recuperarse de problemas que le impidan acceder
al entorno de Windows(R)."
Line02 = "Puede hacer lo siguiente:"
Line03 = "*Rescatar y restaurar los archivos, carpetas o copias de seguridad
utilizando Rescue and Recovery(TM)"
Line04 = "los archivos, carpetas o copias de seguridad utilizando Rescue and
Recovery(TM)"
Line05 = "*Configurar los valores y las contraseñas del sistema"
Line06 = "los valores y las contraseñas del sistema"
Line07 = "*Comunicarse utilizando Internet y enlazar con el sitio de soporte
de Lenovo"
Line08 = "utilizar Internet y enlazar con el sitio de soporte de IBM"
Line09 = "*Solucionar problemas utilizando diagnósticos"
Line10 = "diagnosticar problemas utilizando diagnósticos"
Line11 = "Las funciones pueden variar según las opciones de instalación.
Para obtener información adicional, pulse Introducción
en el menú de Rescue and Recovery."
Line12 = "AVISO:"
Line13 = "Mediante la utilización de este software, queda vinculado por los
términos del Acuerdo de licencia. Para visualizar la licencia,
pulse Ayuda en la barra de herramientas de Rescue and Recovery y,
a continuación, pulse Ver licencia."
Continue = "Continuar"
NowShow = "No mostrar de nuevo"
NoShowCk =0
WelcomeTitle = "Arial Negrita"
WelcomeText = "Arial"
WelcomeBold = "Arial negrita"
```

Los valores siguientes son para las funciones de Ayuda de la barra del título en la interfaz de usuario:

Command0
Página HTML que se iniciará para la página de ayuda base

Command1
Página HTML del Acuerdo de licencia de Lenovo

HELP Ayuda

LICENSE
Licencia

CANCEL
Cancelar

Command0
%sysdrive%Preboot\Helps\en\f_welcom.htm

Command1
%sysdrive%Preboot\Helps\en\C_ILA.htm

Para ocultar completamente la ventana de bienvenida, cambie `NoShowCk=0` a `NoShowCk=1`. Para cambiar los fonts de visualización para el título y el texto de bienvenida, edite las tres últimas líneas de la sección según sus preferencias de diseño.

Nota: No cambie ni suprima las líneas 13 y 14.

En la sección [REBOOT] del archivo PEACCESSIBM*xx*.INI (donde *xx* es la indicación de idioma) puede modificar los valores en las líneas siguientes:

```
NoShowChk=
RebootText=
```

Los dos valores para ″NoShowChk″ son `0` y `1`. El mensaje se puede ocultar cuando un usuario lo desee. Cuando un usuario pulsa en el recuadro de selección cuando se visualiza el mensaje, el valor se establece en `0`. Para que se visualice el mensaje, cambie el valor a `1`. Si es necesario, se puede cambiar la fuente de los mensajes de la sección [REBOOT]. Por ejemplo, este valor se puede establecer de la forma siguiente:

```
RebootText = "Arial"
```

Nota: Las secciones siguientes de PEACCESSIBM*xx*.INI (donde *xx* es la indicación de idioma) están disponible en el archivo, pero no son personalizables: [Messages], [EXITMSG] y [HelpDlg].

Configuración del navegador Opera

El navegador Opera tiene dos archivos de configuración, uno de los cuales contiene la configuración por omisión. El otro es la configuración ″activa″. Un usuario final puede realizar cambios en la configuración activa, pero pierde estos cambios cuando se reinicia Rescue and Recovery.

Para realizar cambios permanentes en el navegador, edite las copias de OPERA6.INI y NORM1.INI que están en %systemdrive%, C, en la siguiente vía de acceso de carpeta: C:\PREBOOT\OPERA\PROFILE. La copia temporal ″activa″ de OPERA6.INI está en la unidad ram (Z:) en el directorio Z:\PREBOOT\OPERA\PROFILE.

Notas:

1. Para obtener, editar y colocar los archivos OPERA6.INI y NORM1.INI, consulte el “Utilización de RRUTIL.EXE” en la página 22.
2. El espacio de trabajo de Opera se ha modificado para proporcionar seguridad mejorada. Como resultado, algunas funciones del navegador se han suprimido.

Correo electrónico

Rescue and Recovery proporciona soporte para el correo electrónico basado en la Web mediante el navegador Opera. Opera proporciona correo electrónico basado en IMAP que se puede habilitar mediante la configuración de empresa grande, pero no está soportado. Para obtener la información de consulta sobre cómo habilitarlo, lea el manual System Administrator’s Handbook en la dirección:

http://www.opera.com/support/mastering/sysadmin/

Inhabilitación de la barra de direcciones

Para inhabilitar la barra de direcciones de Opera, complete el procedimiento siguiente:

1. Obtenga el archivo MINIMAL_TOOLBAR(1).INI de C:\PREBOOT\OPERA\PROFILE\TOOLBAR utilizando el proceso RRUTIL descrito en "Utilización de RRUTIL.EXE" en la página 22.
2. Abra el archivo para editarlo.
3. Localice la sección [Document Toolbar] del archivo.
4. Localice la entrada "Address0".
5. Coloque un signo de punto y coma (; - un delimitador de comentario) delante de la entrada "Address0".

   Nota: Si se detiene aquí y continúa con el paso 7, inhabilita la barra de herramientas de Opera, pero deja el botón Ir y el gráfico de la la barra de herramientas inoperativos. Para eliminar el botón Ir y la barra de herramientas, continúe con el paso 6.
6. Localice las siguientes entradas y, a continuación, coloque un signo de punto y coma delante de cada una:

   ```
   Button1, 21197=Go Zoom2
   ```
7. Guarde el archivo.
8. Ponga el archivo utilizando el proceso RRUTIL descrito en "Utilización de RRUTIL.EXE" en la página 22. La barra de direcciones estará inhabilitada cuando se ejecute Opera.

Personalización de los favoritos

El navegador Opera está configurado para leer los favoritos establecidos en este archivo de la unidad ram: Z:\OPERADEF6.ADR. Este archivo se genera cuando se inicia Rescue and Recovery desde código en la rutina de arranque. La rutina de arranque importa automáticamente los favoritos de Windows Internet Explorer y añade algunos favoritos adicionales. Debido a que este archivo de la unidad ram que se genera durante el arranque es permanente, añade favoritos a Internet Explorer, que se importan automáticamente cuando se inicia el entorno de Rescue and Recovery.

Puede excluir algunos de los favoritos de Internet Explorer, o todos ellos. Para excluir favoritos de usuarios específicos de Windows, haga lo siguiente:

1. Obtenga C:\PREBOOT\STARTUP\OPERA_010.CMD utilizando el proceso RRUTIL descrito en "Utilización de RRUTIL.EXE" en la página 22.
2. Abra el archivo para editarlo.
3. Localice la línea siguiente en el archivo .CMD: PYTHON.EXE.FAVS.PYC Z:\OPERADEF6.ADR
4. Al final de esta línea, especifique entre comillas los nombres de los usuarios de Windows cuyos favoritos desea excluir. Por ejemplo, si desea excluir los favoritos para Todos los usuarios y Administrador, la línea de código será como la siguiente:

   ```
   python.exe favs.pyc z:\Operadef6.adr "Todos los usuarios, Administrador"
   ```
5. Guarde el archivo.
6. Ponga el archivo utilizando el proceso RRUTIL descrito en "Utilización de RRUTIL.EXE" en la página 22.

Si no desea que se visualicen ninguno de los favoritos de Internet Explorer en el navegador proporcionado en el entorno de Rescue and Recovery, haga lo siguiente:

1. Obtenga el archivo C:\PREBOOT\STARTUP\OPERA_010.CMD para editarlo utilizando el proceso RRUTIL descrito en "Utilización de RRUTIL.EXE" en la página 22.

2. Localice la línea siguiente en el archivo .CMD: PYTHON.EXE.FAVS.PYC Z:\OPERADEF6.ADR
3. Haga una de las acciones siguientes:
   a. Escriba REM al principio de la línea, de la forma siguiente:

      ```
      REM python.exe favs.pyc z:\Operadef6.adr
      ```

   b. Suprima la línea de código del archivo.
4. Guarde el archivo.
5. Ponga el archivo de nuevo en su lugar utilizando el proceso RRUTIL descrito en "Utilización de RRUTIL.EXE" en la página 22.

Modificación de los valores del proxy

Para modificar los valores del proxy del navegador Opera, haga lo siguiente:

1. Obtenga el archivo C:\PREBOOT\OPERA\PROFILE\NORM1.INI para editarlo utilizando el proceso RRUTIL descrito en "Utilización de RRUTIL.EXE" en la página 22.
2. Añada la siguiente sección al final del archivo NORM1.INI:

   Nota: La variable [0 o 1] indica que el elemento seleccionado está habilitado (1) o inhabilitado (0).

   ```
   [Proxy]
   Use HTTPS=[0 o 1]
   Use FTP=[0 o 1]
   Use GOPHER=[0 o 1]
   Use WAIS=[0 o 1]
   HTTP Server=[HTTP server]
   HTTPS Server=[HTTPS server]
   FTP Server=[FTP server]
   Gopher Server= [Gopher server]
   WAIS Server Enable HTTP 1.1 for proxy=[0 o 1]
   Use HTTP=[0 o 1]
   Use Automatic Proxy Configuration= [0 o 1]
   Automatic Proxy Configuration URL= [URL]
   No Proxy Servers Check= [0 o 1]
   No Proxy Servers =<Direcciones IP>
   ```

3. Guarde el archivo.
4. Ponga el archivo de nuevo en su lugar utilizando el proceso RRUTIL descrito en "Utilización de RRUTIL.EXE" en la página 22.

Para añadir un proxy HTTP, HTTPS, FTP, Gopher o WAIS, especifique la `=<dirección de proxy>` después de la línea adecuada. Por ejemplo, si la dirección del servidor proxy es http://www.su empresa.com/proxy, la línea HTTP Server tendría el aspecto siguiente:

```
HTTP Server=http://www.su empresa.com/proxy
```

Para añadir el puerto a la entrada, coloque una coma después de la dirección y especifique el número de puerto. Lo mismo es aplicable para los campos ″No Proxy Servers″ y ″Automatic Proxy Configuration URL″.

```
z:\preboot\opera\profile\opera6.ini
```

Habilitación o especificación de la vía de acceso completa de descarga

Existen muchos valores que puede establecer para habilitar la visualización de la ventana ″Guardar como″. El método más sencillo es el siguiente:

1. Obtenga el archivo C:\PREBOOT\OPERA\DEFAULTS\STANDARD_MENU.INI utilizando el proceso RRUTIL descrito en “Utilización de RRUTIL.EXE” en la página 22.
2. En la sección `[Link Popup Menu]`, localice esta serie de caracteres:

   ```
   ;;Item, 50761
   ```
3. Elimine los dos signos de punto y coma y, a continuación, guarde el archivo. Cuando se cierre y vuelva a abrir Rescue and Recovery, un usuario final podrá efectuar una doble pulsación en un enlace y se visualiza la opción ″Guardar destino como″. Esto dará como resultado que se visualice la ventana ″Guardar como″.

   Nota: Los enlaces directos (no enlaces redirigidos) funcionan con el procedimiento anterior. Por ejemplo, si un enlace tiene como destino un script .PHP, Opera guarda sólo el script, no el archivo al que apunta el script.
4. Ponga el archivo de nuevo en la estructura de directorios utilizando el proceso RRUTIL descrito en “Utilización de RRUTIL.EXE” en la página 22.

Para especificar un directorio fijo de descarga, haga lo siguiente:

1. Obtenga el archivo C:\PREBOOT\OPERA\NORM1.INI utilizando el proceso RRUTIL definido descrito en “Utilización de RRUTIL.EXE” en la página 22.
2. En el archivo, localice esta línea:

   ```
   Download Directory=%OpShare%
   ```
3. Cambie `%OpShare%` a la vía de acceso completa del directorio en el que desee que se guarden los archivos descargados.
4. Guarde el archivo NORM1.INI. Cuando se cierre y vuelva a abrir Rescue and Recovery, Opera guardará los archivos descargados en el directorio especificado.
5. Ponga el archivo de nuevo en su lugar utilizando el proceso RRUTIL descrito en “Utilización de RRUTIL.EXE” en la página 22.

Notas:

1. La personalización de la vía de acceso completa para la descarga no permite a los usuarios guardar el archivo de destino, incluso si el enlace está redirigido.
2. El navegador Opera está configurado para descargar sólo los tipos de archivo .ZIP, .EXE y .TXT, y sólo cambia el comportamiento de Opera para estos tipos de archivo. (Existen potencialmente miles de tipos de archivo que utilizan una extensión de archivo de tres letras. Exactamente de la misma forma que el entorno de Rescue and Recovery no pretende ser un sustituto del entorno de Windows, el navegador Opera no pretende sustituir a ningún navegador con todos los servicios. El acceso a Internet se proporciona para ayudar a los usuarios a ponerse en funcionamiento. El número de tipos de archivo reconocidos es necesariamente limitado. Para la finalidad del rescate y la recuperación, deben ser suficientes los archivos .ZIP, .EXE y .TXT. Si es necesario transferir otro tipo de archivo, los mejores resultados se consiguen creando un archivo .ZIP, que se puede extraer posteriormente.)
3. Los tipos de archivo se reconocen por el tipo mime en lugar de por la extensión de archivo. Por ejemplo, si un archivo .TXT se nombra teniendo como extensión .EUY, el archivo seguirá siendo abierto en el navegador Opera como un archivo de texto.

Adición de una extensión específica de archivo a la lista de archivos descargables

Puede realizar adiciones a la lista de archivos que se pueden descargar mediante el navegador de Rescue and Recovery. Para realizar adiciones a la lista, complete el procedimiento siguiente:

1. Asegúrese de que Opera esté cerrado y de que todas las ventanas de Opera estén cerradas, incluyendo los archivos de ayuda de Rescue and Recovery.
2. Obtenga el archivo C:\PREBOOT\OPERA\NORM1.INI utilizando el proceso RRUTIL descrito en "Utilización de RRUTIL.EXE" en la página 22.
3. Localice la sección [File Types] del archivo.
4. Utilice la función de búsqueda para descubrir si la extensión de archivo que desea está en la lista pero no funciona; a continuación, realice una de las acciones siguientes:
   - Si encuentra la extensión, pero los archivos con dicha extensión no funcionan correctamente, complete los pasos siguientes:
     a. Cambie el valor que aparece a continuación de la extensión de 8 a 1. (Un valor de 8 indica al navegador que ignore el archivo. Un valor de 1 indica al navegador que guarde el archivo.) Por ejemplo, cambie lo siguiente:

        ```
        video/mgpeg=8,,,,mpeg,mpg,mpe,m2v,m1v,mpa,|
        ```

        a

        ```
        video/mgpeg=1,,,,mpeg,mpg,mpe,m2v,m1v,mpa,|
        ```

     b. Desplácese hasta la sección [File Types Extension] del archivo NORM1.INI y, a continuación, busque el tipo mime del archivo. Por ejemplo, busque lo siguiente: VIDEO/MPEG=,8
     c. Cambie el valor ,8 a lo siguiente:

        ```
        %opshare%\,2
        ```

        Nota: Si el valor ya está establecido de la forma especificada, no cambie el valor.
     d. Guarde el archivo y luego copie el archivo en OPERA6.INI; a continuación, reinicie Rescue and Recovery para que los cambios sean efectivos.
   - Si la extensión no está presente y los archivos del tipo deseado no funcionan correctamente, haga lo siguiente:
     a. En la sección [File Types Extension] de NORM1.INI, localice la entrada mime temporal. A continuación se muestra un ejemplo: temporary=1,,,,lwp,prz,mwp,mas,smc,dgm,|
     b. Añada la extensión del tipo de archivo a la lista. Por ejemplo, si desea añadir .CAB como una extensión reconocida, añádala según la siguiente entrada de muestra:

        ```
        temporary=1,,,,lwp,prz,mwp,mas,smc,dgm,cab,|
        ```

        Nota: La coma y la barra vertical al final son esenciales para que este valor funcione. Si se omite cualquiera de los dos, todos las extensiones de archivo de la lista se inhabilitarán.
     c. Guarde el archivo en la vía de acceso de directorio C:\TEMP\.
     d. Copie el archivo en OPERA6.INI.
     e. Reinicie el espacio de trabajo de Rescue and Recovery para que los cambios sean efectivos.

Modificación del comportamiento de archivos con extensiones específicas

Puede modificar el comportamiento de archivos sustituyendo valores en el archivo NORM1.INI. Para cambiar el comportamiento de los archivos por la extensión, realice lo siguiente:

1. Cierre Opera y todas las ventanas activas de Opera, incluyendo los archivos de ayuda.
2. Abra el archivo PREBOOT\OPERA\NORM1.INI para editarlo utilizando el proceso RRUTIL descrito en "Utilización de RRUTIL.EXE" en la página 22.

3. Localice la sección [File Types] del archivo y, a continuación, busque la extensión con la que desea trabajar. Por ejemplo, desea que todos los archivos .TXT se guarden en la carpeta IBMSHARE.
4. Busque la entrada siguiente: TEXT/PLAIN=2,,,,TXT,|

   Nota: Un valor de 2 indica al navegador que visualice el texto en Opera. Un valor de 1 indica al navegador que guarde el archivo de destino en la carpeta IBMSHARE.
5. Continuando con el ejemplo de .TXT, cambie la línea para que tenga el siguiente aspecto:

   ```
   TEXT/PLAIN=1,,,,TXT,|
   ```
6. Guarde el archivo y póngalo de nuevo en su lugar utilizando el proceso RRUTIL tal como se describe en "Utilización de RRUTIL.EXE" en la página 22.
7. Reinicie el espacio de trabajo de Rescue and Recovery para que los cambios sean efectivos.

Adición de una dirección IP estática

Para añadir una dirección IP estática, necesita cambiar los archivos siguientes.

1. Obtenga el archivo \MININT\SYSTEM32 WINBOM.INI utilizando el proceso RRUTIL descrito en "Utilización de RRUTIL.EXE" en la página 22.
2. Añada la sección [WinPE.Net] antes de [PnPDriverUpdate] en el archivo WINBOM.INI. Por ejemplo, considere el archivo siguiente: WINBOM.INI

   ```
   [Factory]
   WinBOMType=WinPE
   Reseal=No
   [WinPE]
   Restart=No
   [PnPDriverUpdate]
   [PnPDrivers]
   [NetCards]
   [UpdateInis]
   [FactoryRunOnce]
   [Branding]
   [AppPreInstall]
   ```

   Debe añadir las líneas siguientes a la sección [WinPE.Net].

   ```
   [WinPE.Net]
   Gateway=9.44.72.1
   IPConfig =9.44.72.36
   StartNet=Yes
   SubnetMask=255.255.255.128
   ```

Tabla 7. Entradas de dirección IP estática

Entrada	Descripción
Gateway	Especifica la dirección IP de un direccionador IP. La configuración de una pasarela por omisión crea una ruta por omisión en la tabla de direccionamiento IP. **Sintaxis:** Gateway = *xxx.xxx.xxx.xxx*
IPConfig	Especifica la dirección IP que Windows PE utiliza para conectar con una red. **Sintaxis:** IPConfig = *xxx.xxx.xxx.xxx*

Tabla 7. Entradas de dirección IP estática (continuación)

Entrada	Descripción
StartNet	Especifica si se deben iniciar los servicios de red. **Sintaxis:** StartNet = *Yes* | *No*
SubnetMask	Especifica un valor de 32 bits que permite al receptor de paquetes IP distinguir las partes del ID de red y del ID de sistema principal de la dirección IP. **Sintaxis:** SubnetMask = *xxx.xxx.xxx.xxx*

3. Obtenga el archivo PREBOOT\IBMWORK NETSTART.TBI utilizando el proceso RRUTIL descrito en "Utilización de RRUTIL.EXE" en la página 22.
4. Cambie

   ```
   factory -minint
   ```

   a

   ```
   factory -winpe
   ```
5. Elimine los comentarios de las líneas siguientes:

   ```
   regsvr32 /s netcfgx.dll
   netcfg -v -winpe
   net start dhcp
   net start nla
   ```
6. Ponga los archivos \IBMWORK NETSTART.TBI y \MININT\SYSTEM32 WINBOM.INI de nuevo en su lugar utilizando el proceso RRUTIL descrito en "Utilización de RRUTIL.EXE" en la página 22.

Modificación de la resolución de vídeo

Puede modificar la resolución de vídeo cambiando los valores por omisión de la resolución del área previa al escritorio de 800 × 600 × 16 bits. Para modificar los valores, haga lo siguiente:

1. Obtenga el archivo MININT\SYSTEM32\WINBOM.INI utilizando el proceso RRUTIL descrito en "Utilización de RRUTIL.EXE" en la página 22.
2. En el archivo WINBOM.INI, añada las entradas siguientes:

   ```
   [ComputerSettings]
   DisplayResolution=800x600x16 o 1024x768x16
   En el archivo
   preboot\ibmwork\netstart.tbi, cambie factory-minint a factory-winpe
   ```

   Cuando se inicie el entorno de Rescue and Recovery, verá una ventana adicional durante el arranque que tiene el título de ″Preinstalación de fábrica″. Además, los colores se reducirán de miles a 256.
3. Ponga de nuevo en su lugar el archivo MININT\SYSTEM32\WINBOM.INI utilizando el proceso RRUTIL descrito en "Utilización de RRUTIL.EXE" en la página 22.

Aplicaciones de arranque

El entorno de Windows PE de Rescue and Recovery tiene la capacidad de dar soporte a scripts, programas o programas personalizados de arranque. Estos scripts o programas se procesarán antes de que el entorno de Windows PE de Rescue and Recovery alcance la página principal de la interfaz de PE.

El directorio donde colocar el script o los programas es Preboot\Startup. Los scripts o programas de este directorio se procesarán alfanuméricamente. Por lo tanto, un script denominado A.BAT se procesaría antes que 1.EXE.

Para colocar un script o programa en este directorio, haga lo siguiente:

1. Obtenga RRUTIL del sitio de las Herramientas de administración de Rescue and Recovery en la dirección:

   www.lenovo.com/ThinkVantage
2. Cree un directorio temp
3. En el directorio \Temp cree el siguiente árbol de directorios, \preboot\startup
4. Coloque el script o programa en la vía de acceso \temp\preboot\startup
5. Desde el indicador de la línea de mandatos, escriba RRUTIL –p \Temp
6. 6) Para verificar que el script o programa se ha copiado satisfactoriamente, escriba RRUTIL –g en la línea de mandatos. Esto generará un archivo denominado getlist.txt.
7. 7) Examine el contenido de getlist.txt para el directorio \preboot\startup. El script o programa se debe listar bajo este árbol.

Contraseñas

Existen cuatro opciones de contraseña disponibles en el Área previa al escritorio. Son las siguientes:

- Contraseña del Área previa al escritorio o maestra
- ID de usuario y contraseña o frase de paso
- Contraseña de copia de seguridad
- Ninguna contraseña

Contraseña del Área previa al escritorio o maestra

Puede establecer una contraseña independiente del Área previa al escritorio. Esta contraseña se establece mediante la interfaz de la línea de mandatos, y es la única opción de contraseña disponible si no está instalado Client Security Solution.

Puede crear esta contraseña del Área previa al escritorio utilizando el mandato siguiente: C:\Archivos de programa\IBM ThinkVantage\Client Security Solution\pe_setupmasterpwde.exe.

Los parámetros de este mandato son:

Tabla 8.

Parámetro	**Descripción**
create password	Este parámetro crea la propia contraseña.
verify password	Este parámetro verifica que la contraseña sea válida y de que se pueda utilizar.
change contraseñaActual *nuevaContraseña*	Este parámetro le permite cambiar la contraseña actual por otra.
exists	Este parámetro comprueba si la contraseña existe
silent	Este parámetro oculta todos los mensajes
setmode values	0 = no es necesaria ninguna autentificación 1 = es necesaria una autentificación específica de usuario 2 = es necesario una contraseña maestra

Nota: Un usuario con limitaciones no puede cambiar la contraseña; un administrador puede restablecer la contraseña para un usuario con limitaciones.

ID de usuario y contraseña o frase de paso

Esta opción utiliza el código de Client Security Solution para la gestión de las contraseñas y frases de paso. El inicio de sesión de Client Security solicitará al usuario esta contraseña o frase de paso al arrancar en el Área previa al escritorio. Esto proporciona una mejor seguridad para un entorno de varios usuarios. Si un usuario inicia sesión utilizando el inicio de sesión, se permitirá a dicho usuario acceder sólo a sus archivos, no a los archivos de otro usuario.

Esta opción se puede establecer en la GUI de CSS o mediante scripts XML.

Contraseña de copia de seguridad

Se puede establecer la contraseña de copia de seguridad mediante la GUI Establecer contraseña o mediante la interfaz de la línea de mandatos rrcmd, especificando backup. A continuación se muestran algunos ejemplos:

```
rrcmd backup location=L name=micopiaseguridad password=pase
rrcmd basebackup location=L name=copiaseguridadbase password=pase
rrcmd sysprepbackup location=L name="Copia de seguridad Sysprep" password=pase
```

Sin contraseña

Esta opción no utiliza ninguna autentificación y permite al usuario entrar en el Área previa al escritorio sin utilizar ninguna contraseña

Acceso de contraseña de ID

Existen tres opciones de acceso de contraseña:

- Contraseña maestra
- ID de usuario y contraseña o frase de paso
- Sin contraseña

Contraseña maestra

La contraseña maestra es una única contraseña que le permite acceder al Área previa al escritorio y a las copias de seguridad. Se establece utilizando la interfaz de la línea de mandatos y es la única opción de contraseña si Client Security Solution no está instalado.

ID de usuario y contraseña o frase de paso

Esta opción utiliza el código de Client Security Solution para la gestión de las contraseñas o frases de paso. Client Security Solution GINA solicitará al usuario esta contraseña o frase de paso al arrancar en el Área previa al escritorio. Esto proporciona una mejor seguridad para un entorno de varios usuarios. Si un usuario inicia sesión utilizando GINA, se permitirá a dicho usuario acceder solamente a sus archivos de usuario, no a los de los demás usuarios.

Nota: Esto también incluye la información en el archivo de volumen cifrado de SecureDrive PrivateDisk del usuario.

Esta opción se puede establecer mediante la interfaz de la línea de mandato o la GUI.

Sin contraseña

Esta opción no utiliza ninguna autorización y permite al usuario entrar en el Área previa al escritorio sin utilizar ninguna contraseña.

Tipo de restauración

A continuación se listan los métodos para la restauración de archivos:

- Rescate de archivos
- Restauración de un único archivo
- Sistema operativo y aplicaciones
- Rejuvenecimiento
- Restauración completa
- Contenido de fábrica/Image Ultra Builder

Nota: Rescue and Recovery no puede capturar credenciales colocadas en la antememoria para un usuario de dominio después de una restauración.

Rescate de archivos (antes de cualquier restauración)

Esta función solicita al usuario la ubicación del almacenamiento de la copia de seguridad y, a continuación, el usuario selecciona una copia de seguridad. A continuación, ThinkVantage Rescue and Recovery debe visualizar los archivos a los que el usuario que ha iniciado la sesión está autorizado a acceder. A continuación, el usuario selecciona los archivos y/o las carpetas que se deben rescatar. El sistema visualizará las ubicaciones disponibles para los archivos que se deben rescatar, excluyendo la unidad de disco duro local. El usuario selecciona un destino con espacio suficiente y el sistema restaura los archivos.

Restauración de un único archivo

Esta función solicita al usuario la ubicación del almacenamiento de la copia de seguridad y, a continuación, el usuario selecciona una copia de seguridad. A continuación, ThinkVantage Rescue and Recovery debe visualizar los archivos a los que el usuario que ha iniciado la sesión está autorizado a acceder. A continuación, el usuario selecciona los archivos y/o carpetas que se deben rescatar y el sistema restaurará estos archivos y/o carpetas en sus ubicaciones originales.

Sistema operativo y aplicaciones

Esta función proporciona al usuario la opción de seleccionar una copia de seguridad; a continuación, el sistema suprime los archivos definidos por las normas de osfilter.txt. Luego restaura los archivos definidos por OSFILTER.TXT a partir de la copia de seguridad seleccionada. Además, existen opciones en el archivo tvt.txt que pueden especificar que se ejecute un programa antes de una restauración o después de una restauración. Consulte los valores y parámetros de TVT.

Notas:

1. El sistema operativo y las aplicaciones siempre utilizan la Persistencia de contraseña.
2. La restauración del sistema operativo y de las aplicaciones no está disponible desde la copia de seguridad en CD/DVD.

Puede añadir tareas personalizadas para que se ejecuten antes y después de las copias de seguridad y de las restauraciones. Consulte el Apéndice B, “Parámetros y valores de TVT.TXT”, en la página 149 para ver los valores de copia de seguridad y de restauración.

Rejuvenecimiento

Cuando seleccione rejuvenecer el sistema, el programa Rescue and Recovery optimizará el rendimiento del sistema realizando una nueva copia de seguridad incremental y, a continuación, defragmentando el disco duro y las copias de seguridad. Acto seguido, restaurará los valores y los datos seleccionados a partir de una copia de seguridad de su elección. Las operaciones de rejuvenecimiento le ayudan a eliminar virus, adware y spyware al mismo tiempo que mantienen los valores y datos actuales. Es posible que estas operaciones lleven algún tiempo.

Para rejuvenecer el sistema, complete el procedimiento siguiente:

1. En la interfaz de Rescue and Recovery, pulse el icono **Restaurar el sistema a partir de una copia de seguridad**. Se visualizará la pantalla Restaurar el sistema.
2. En la pantalla Restaurar el sistema, seleccione **Rejuvenecer el sistema**.
3. Seleccione la unidad y la copia de seguridad que desea utilizar para rejuvenecer el sistema completando el procedimiento siguiente:
   a. Seleccione la unidad adecuada en el menú desplegable de unidades disponibles. Los archivos de copia de seguridad de la unidad seleccionada se visualizan en la interfaz de Rescue and Recovery.
   b. Seleccione el archivo de copia de seguridad que desee utilizar para rejuvenecer el sistema.
   c. Pulse **Siguiente**.
   d. Confirme que la copia de seguridad seleccionada es la que desea utilizar para rejuvenecer el sistema y, a continuación, pulse **Siguiente** para empezar el proceso de restauración. Se le recuerda que no apague el sistema durante esta operación.
   e. Pulse **Aceptar** para continuar. Se visualizará una barra de progreso. Esta operación llevará algún tiempo.

Puede añadir tareas personalizadas para que se ejecuten antes o después del rejuvenecimiento. Consulte el Apéndice B, “Parámetros y valores de TVT.TXT”, en la página 149 para ver los valores de rejuvenecimiento

Nota: Es posible que sea necesario volver a instalar las aplicaciones instaladas o desinstaladas después de la creación de la copia de seguridad seleccionada a fin de que éstas funcionen correctamente.
Atención: Asegúrese de que el sistema esté conectado a una fuente de alimentación de CA antes de inicializar un procedimiento de copia de seguridad, restauración, rejuvenecimiento o archivado. Si no es así, esto puede dar como resultado la pérdida de datos o un fallo irrecuperable del sistema.

Restauración completa

Esta función suprime todos los archivos de la unidad local y, a continuación, restaura los archivos de la copia de seguridad seleccionada. Si se ha seleccionado la persistencia de contraseña, se restaurará la contraseña más reciente disponible.

Contenido de fábrica/Image Ultra Builder (IUB)

Esta función borra el disco duro y vuelve a instalar todo el software preinstalado de fábrica.

Persistencia de contraseña

La tabla siguiente muestra las consideraciones que se deben tener en cuenta al seleccionar o no la Persistencia de contraseña.

Tabla 9. Consideraciones sobre la Persistencia de contraseña

Asunto	**Impacto si la Persistencia de contraseña está habilitada**
Si un usuario inicia la sesión en una copia de seguridad antigua con la cuenta y la contraseña actuales, no funcionará ninguno de los archivos ni carpetas del sistema cifrado de archivos porque estos archivos se cifraron con la cuenta y contraseña original, no con la cuenta y contraseña persistente.	• El usuario perderá los datos del Sistema cifrado de archivos • No puede utilizar conjuntamente el sistema cifrado de archivos y la Persistencia de contraseña.
Si el usuario no existía en esa copia de seguridad determinada, no tendrá ninguno de sus archivos o carpetas de usuario. No existirá ninguno de los Favoritos de Internet Explorer ni los datos de las aplicaciones.	• Se pierden los Valores de los documentos del ID de usuario • Potencial pérdida de datos
La supresión del usuario en las cuentas y contraseñas actuales eliminará su información de autentificación de todas las copias de seguridad.	• El usuario no tendrá acceso a los datos
Si un gestor o un administrador de red deseara suprimir el acceso de varios ex-empleados y deseara restaurar a la copia de seguridad base para restablecer el sistema a fin de eliminar todas las cuentas de autentificación de los empleados, los empleados seguirían teniendo acceso con la Persistencia de contraseña.	• Va contra las recomendaciones de las prácticas y recomendaciones de mantenimiento de ID de usuario de Microsoft.

Al restaurar desde una unidad de disco duro local, la contraseña actual se utilizará cuando la Persistencia de contraseña esté seleccionada. Al restaurar desde USB o desde la red, se utilizará la contraseña de la copia de seguridad más reciente.

Restablecimiento de la contraseña de hardware

El entorno de Restablecimiento de la contraseña de hardware se ejecuta independientemente de Windows y le permitirá restablecer contraseñas de disco duro y de encendido olvidadas. La identidad del usuario se establece respondiendo a una serie de preguntas que el usuario ha creado al registrase. Es recomendable crear, instalar y registrar este entorno seguro lo antes posible, antes de que se olvide una contraseña. No puede restablecer contraseñas de hardware olvidadas hasta después de que se haya registrado. Este soporte de recuperación está soportado solamente en sistemas ThinkCentre y ThinkPad seleccionados.

La creación de este entorno no le ayuda a recuperarse de contraseñas de Windows o de contraseñas asociadas con el espacio de trabajo de Rescue and Recovery que se hayan olvidado. Creando este entorno, está añadiendo un dispositivo de arranque adicional al menú Device Menu (Dispositivo de arranque), desde el que puede restablecer las contraseñas de hardware olvidadas. Puede acceder a este menú pulsando F12 cuando se le solicite la contraseña de encendido.

Existen tres pasos integrantes de la configuración del despliegue de contraseña:

1. Creación del paquete
2. Despliegue del paquete
3. Registro

Establezca una contraseña de administrador o de supervisor en el BIOS antes de empezar este procedimiento. Si no tiene establecida la contraseña de administrador o de supervisor del BIOS, el entorno no será lo más seguro posible. Todos los sistemas en los que planea desplegar el paquete de restablecimiento de contraseña deben tener contraseña de supervisor. Cuando complete este procedimiento, la contraseña de encendido y la contraseña de disco duro serán la misma. Este procedimiento está diseñado para ayudarle a completar la tarea de creación del entorno seguro y para ayudarle a restablecer las contraseñas olvidadas después de que se haya creado el entorno seguro.

Creación del paquete

Para crear un entorno seguro, haga lo siguiente:

1. En la aplicación de instalación de restablecimiento de contraseña de hardware, marque el botón de selección Crear entorno seguro para restablecer contraseñas de hardware.
2. Pulse Aceptar. Se abrirá la ventana Contraseña de supervisor del BIOS.
3. En el campo Entrar contraseña de supervisor, especifique la contraseña de administrador o supervisor. Ésta es la contraseña de administrador o supervisor que ha establecido anteriormente en el BIOS para proteger los valores de hardware.
4. Pulse Aceptar. Se abrirá la ventana Crear clave.
5. En el área de generación de claves, realice una de las acciones siguientes:

   La primera vez que cree este entorno seguro, deberá crear una nueva clave. Una clave es una característica de seguridad utilizada para autentificar la identidad del usuario. Los intentos posteriores de crear un entorno seguro le darán la opción de utilizar la misma clave que ha creado en el intento inicial si selecciona exportarla o crear una clave distinta. Si está creando este entorno sólo para un sistema, es recomendable generar una nueva clave. Puede optar a generar una clave cada vez que cree un nuevo sistema operativo seguro. Sin embargo, esta opción requiere que vuelva a realizar el procedimiento de registro en cada máquina. Si se utiliza la misma clave, no es necesario volver a realizar el registro. Si está creando este entorno para varios sistemas, es posible que desee utilizar la misma clave. Sin embargo, es recomendable que si va a utilizar la misma clave, debe almacenar la clave en una ubicación segura.

   En el área de generación de claves, realice una de las acciones siguientes:

   - Si es la primera vez que crea una clave y planea crear el entorno seguro sólo en este sistema, marque el botón de selección Generar nueva clave.
   - Si es la primera vez que crea una clave y desea crear un entorno seguro que se pueda desplegar a otros sistemas, marque el botón de selección Generar nueva clave. A continuación, marque el recuadro de selección Exportar clave a archivo. Utilice el botón Examinar para definir donde desea que se almacene la clave.
   - Si ya ha creado una clave y desea utilizar la clave para crear un entorno seguro que pueda desplegar en otros sistemas, marque el botón de selección Importar clave de archivo. Utilice el botón Examinar para definir donde está ubicada la clave que desea utilizar. Necesitará la clave creada en la opción anterior.

Configure un sistema donante para cada tipo de sistema soportado cuando realice el despliegue en un Thinkpad, Thinkcentre, y por idioma, por ejemplo, francés, alemán, japonés. El propósito es asegurar el sistema operativo que está basado en la partición Rescue and Recovery y que será distinto para cada sistema.

6. En el área de instalación, deseleccione el recuadro de selección Instalar automáticamente el restablecimiento de contraseña de hardware.
7. Pulse **Aceptar**.
8. Pulse **Aceptar** en un recuadro de diálogo que le informa acerca de que la característica de Contraseña de hardware no se habilitará en este sistema hasta que se haya ejecutado el paquete de instalación.

   Para buscar la vía de acceso al archivo ejecutable, escriba cd %rr%\rrcd\passwordreset\pwdreset.exe en el indicador de la línea de mandatos.

Despliegue del paquete

Utilice el soporte de distribución existente de la empresa para desplegar el paquete creado.

Registro

Para registrar el restablecimiento de contraseña, haga lo siguiente:

1. Ejecute pwdreset.exe
2. Pulse Aceptar para reiniciar el sistema. El sistema se reiniciará y le solicitará que especifique las contraseñas del BIOS. Especifique las contraseñas del BIOS y, a continuación, especifique **Intro**. El sistema se reiniciará en el entorno seguro donde se abrirá la ventana Bienvenido a Restablecimiento de contraseña de hardware.
3. Marque el botón de selección **Configurar restablecimiento de hardware** si ésta es la primera vez que crea el entorno seguro o si desea volver a registrar el sistema y los discos duros.
4. Pulse **Siguiente**. Se abrirá la ventana Configurar discos duros.
5. En el área del número de serie del sistema, marque el recuadro de selección Configurar situado junto al sistema que desea configurar.
6. Pulse **Siguiente**. Se abrirá la ventana Especificar nueva contraseña de encendido.
7. En el campo **Nueva contraseña de encendido**, escriba la contraseña de encendido que desee utilizar. Si ya tiene una contraseña de encendido, se restablecerá a la contraseña que ha entrado en el campo. Además, la contraseña de disco duro también se establecerá a la misma contraseña.
8. Pulse **Siguiente**. Se abrirá la ventana Crear preguntas y respuestas de seguridad.
9. En cada uno de los tres campos de preguntas, especifique la contraseña de encendido que desee utilizar. Si ya tiene una contraseña de encendido, se restablecerá a la que ha especificado en el campo. Además, la contraseña de disco duro también se establecerá a la misma contraseña.
10. En cada uno de los tres campos de respuestas, escriba la respuesta a la pregunta. Será necesario que conozca cada respuesta en el caso de que olvide la contraseña de encendido e intente restablecerla.
11. Pulse **Siguiente** y, a continuación, pulse **Finalizar**. El sistema se reiniciará en el entorno de Windows.

A continuación se muestran los mensajes de error del instalador del restablecimiento de contraseña de hardware. Los dos primeros son títulos genéricos, utilizados en combinación con el resto de los mensajes. En ambos casos, se recomienda que vuelva a instalar el producto.

- **IDS_STRING_ERR** ″Error″
- **IDS_STRING_ERR_INT** ″Errror interno″
- **IDS_STRING_ERR_CMDLINE** ″No se ha reconocido la opción de la línea de mandatos que ha especificado.\n\nUso: scinstall [/postenroll | /biosreset | /newplanar]″
- **IDS_STRING_ERR_NOTSUPPORTED**

  El restablecimiento de contraseña de hardware no está soportado en este sistema.
- **IDS_STRING_ERR_MEM**

  Este sistema no tiene memoria suficiente para ejecutar la característica de restablecimiento de contraseña de hardware.
- **IDS_STRING_ERR_ENVAR**

  Falta una variable de entorno necesaria. Rescue and Recovery 3.0 (o superior) debe estar instalado a fin de poder utilizar la característica de restablecimiento de contraseña de hardware.
- **IDS_STRING_ERR_MISSINGDLL**

  Falta una DLL necesaria. Rescue and Recovery 3.0 (o superior) debe estar instalado a fin de poder utilizar la característica de restablecimiento de contraseña de hardware.
- **IDS_STRING_ERR_BIOSMAILBOX**

  La actualización del BIOS para instalar la característica de restablecimiento de contraseña de hardware ha fallado. Apague el sistema; a continuación, reinicie y vuelva a intentar la instalación de restablecimiento de contraseña de hardware.
- **IDS_STRING_ERR_INSTALLRETRY**

  Esta operación no se ha completado satisfactoriamente. Para intentarlo de nuevo, apague el sistema, reinicie y ejecute de nuevo la instalación de restablecimiento de contraseña de hardware.
- **IDS_STRING_ERR_INSTALLPUNT**

  Esta operación no se ha completado satisfactoriamente. Para solucionar el problema, consulte al administrador del sistema o la documentación de Rescue and Recovery para obtener más detalles.

Capítulo 4. Personalización de Client Security Solution

Este capítulo utiliza términos definidos por Trusted Computing Group (TCG) en relación al Módulo de plataforma fiable. Para obtener una información más detallada de estos términos, consulte el siguiente sitio para ver referencias y definiciones:

http://www.trustedcomputinggroup.org/

Ventajas del chip de seguridad incorporado/Módulo de plataforma fiable

Un Módulo de plataforma fiable es un chip de seguridad incorporado diseñado para proporcionar funciones relacionadas con la seguridad para el software que lo utiliza. El chip de seguridad incorporado se instala en la placa madre de un sistema y se comunica mediante un bus de hardware. Los sistemas que incorporan un Módulo de plataforma fiable pueden crear claves de cifrado y cifrarlas de forma que sólo puedan ser descifradas por el mismo Módulo de plataforma fiable. Este proceso, a menudo denominado *empaquetado* de una clave, ayuda a proteger la clave evitando que se revele. En un sistema con un Módulo de plataforma fiable, la clave de empaquetado maestra, denominada Clave raíz de almacenamiento (SRK - Storage Root Key), se almacena en el propio Módulo de plataforma fiable, de forma que la parte privada de la clave nunca queda expuesta. El chip de seguridad incorporado también puede almacenar otras claves de almacenamiento, claves de firma, contraseñas y otras pequeñas unidades de datos. Sin embargo, existe una capacidad limitada de almacenamiento en el Módulo de plataforma fiable, se forma que la SRK se utiliza para cifrar otras claves para el almacenamiento fuera del chip. Debido a que la SRK nunca deja el chip de seguridad incorporado, forma la base para el almacenamiento protegido.

Cuando se necesitan los datos protegidos por el Módulo de plataforma fiable, los datos protegidos pasan al entorno de hardware incorporado seguro para su proceso. Después de una autentificación y una descodificación satisfactorias, los datos desprotegidos se pueden utilizar en el sistema.

Los sistemas que incorporan un Módulo de plataforma fiable son resistentes a los ataques de la misma forma que cualquier hardware es más resistente al ataque que el software. Esto es especialmente importante cuando se aprovechan las claves de cifrado. Las partes privadas de pares de claves asimétricas se mantienen segregadas de la memoria controlada por el sistema operativo. El Módulo de plataforma fiable utiliza sus propios circuitos lógicos y firmware interno para procesar las instrucciones, no confía en el sistema operativo y no está sujeto a vulnerabilidades exteriores del software.

Ningún sistema puede proporcionar una seguridad perfecta, incluyendo los sistemas que utilizan la tecnología del Módulo de plataforma fiable. El chip de seguridad incorporado está diseñado para resistir la manipulación no autorizada o el análisis electrónico. Sin embargo, la realización de la clase de análisis necesario para revelar secretos protegidos mediante el Módulo de plataforma fiable requiere acceso físico a la máquina y hardware especializado adicional, haciendo que los secretos de una plataforma habilitada con el chip de seguridad sean mucho más seguros que aquellos en un sistema que sólo incluya el software. Si se aumenta la

dificultad de sustraer secretos de los sistemas, se ayuda a aumentar el nivel general de seguridad para el individuo o la empresa.

El chip de seguridad incorporado es un proceso opcional y requiere un Administrador de Client Security Solution. Ya sea para el usuario individual o para un departamento de TI de una empresa, se debe inicializar el Módulo de plataforma fiable. Las operaciones subsiguientes, como por ejemplo la capacidad de recuperarse de un fallo del disco duro o la sustitución de la placa del sistema, también están restringidas al Administrador de Client Security Solution.

Cómo Client Security Solution gestiona las claves de cifrado

El mecanismo interno de Client Security Solution se describe mediante las dos actividades principales de despliegue; Tomar propiedad y Registrar usuario. Al ejecutar el Asistente de configuración de Client Security por primera vez, los procesos Tomar propiedad y Registrar usuario se realizan durante la inicialización. El ID de usuario de Windows específico que ha completado el Asistente de configuración de Client Security es el Administrador de Client Security Solution y se registra como un usuario activo. A todos los demás usuarios que inicien sesión en el sistema se les requerirá que se registren en Client Security Solution.

- **Tomar propiedad - asignar administrador de Client Security Solution**

  Se asigna un único ID de usuario Administrador de Windows al único Administrador de Client Security Solution del sistema. Las funciones administrativas de Client Security Solution se deben realizar mediante este ID de usuario. La autorización del Módulo de plataforma fiable es la contraseña de Windows de este usuario o la frase de paso de Client Security.

  Nota: La única forma de recuperar una contraseña de Administrador o frase de paso de Client Security Solution es desinstalar el software con los permisos válidos de Windows o borrar el chip de seguridad en el BIOS. De cualquiera de las dos maneras se perderán los datos protegidos mediante las claves asociadas con el Módulo de plataforma fiable. Client Security Solution también proporciona un mecanismo opcional que permite la autorecuperación de una contraseña o frase de paso olvidada basándose en un reto pregunta-respuesta que forma parte de la función Registrar usuario. El Administrador de Client Security Solution toma la decisión sobre si utilizar esta función.

- **Registrar usuario**

  Una vez que se haya completado el proceso Tomar propiedad y se haya creado un Administrador de Client Security Solution, se podrá crear una clave base de usuario para almacenar de forma segura credenciales para el usuario de Windows que actualmente ha iniciado la sesión. Este diseño permite que múltiples usuarios se registren en Client Security Solution y aprovechen el único Módulo de plataforma fiable. Las claves de usuario están protegidas mediante el chip de seguridad, pero en realidad se almacenan fuera del chip en la unidad de disco duro. A diferencia de otras tecnologías de seguridad, este diseño crea espacio de disco duro como factor de almacenamiento con limitaciones en lugar de memoria real incorporada en el chip de seguridad. Con este diseño, el número de usuarios que pueden aprovechar el mismo hardware seguro se aumenta considerablemente.

Tomar propiedad

La raíz de fiabilidad de Client Security Solution es la Clave raíz del sistema (SRK - System Root Key). Esta clave asimétrica que no se puede migrar se genera en el entorno seguro del Módulo de plataforma fiable y nunca se expone al sistema. La

autorización para aprovechar la clave se deriva a través de la cuenta de Administrador de Windows durante el mandato "TPM_TakeOwnership". Si el sistema está aprovechando una frase de paso de Client Security, la frase de paso de Client Security para el administrador de Client Security Solution será la autorización del Módulo de plataforma fiable; de lo contrario, será la contraseña de Windows del Administrador de Client Security Solution.

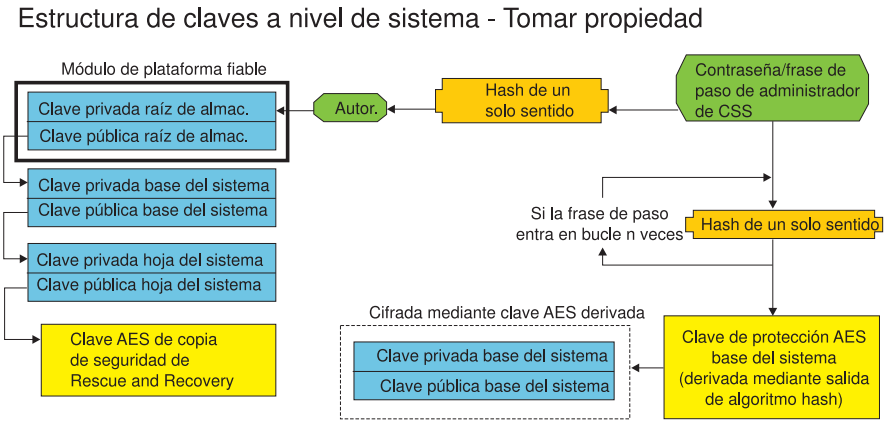

Figura 1.

Una vez que se haya creado la SRK para el sistema, se podrán crear otros pares de claves y estos se podrán almacenar fuera del Módulo de plataforma fiable, pero envueltos o protegidos mediante las claves basadas en hardware. Debido a que el Módulo de plataforma fiable que incluye la SRK es hardware y el hardware puede resultar dañado, es necesario un mecanismo de recuperación para garantizar la recuperación de los datos en caso de que se produzcan daños en el sistema.

Para recuperar un sistema se crea la Clave base del sistema. Esta clave de almacenamiento asimétrica que se puede migrar permitirá al Administrador de Client Security Solution la recuperación de un cambio de la placa del sistema o la migración planificada a otro sistema.

A fin de proteger la Clave base del sistema pero permitir que sea accesible durante el funcionamiento normal o durante la recuperación, se crean y protegen dos instancias de la clave mediante dos métodos distintos. En primer lugar, se cifra la Clave base del sistema con una clave simétrica AES que se deriva sabiendo la contraseña del Administrador de Client Security Solution o la frase de paso de Client Security. Esta copia de la Clave de recuperación de Client Security Solution se utiliza exclusivamente a fin de realizar la recuperación de un Módulo de plataforma fiable borrado o de una placa del sistema sustituida debido a un fallo de hardware.

La segunda instancia de la Clave de recuperación de Client Security Solution es empaquetada por la SRK para importarla en la jerarquía de claves. Esta doble instancia de la Clave base del sistema permite al Módulo de plataforma fiable proteger los secretos vinculados al mismo más abajo durante la utilización normal y permite la recuperación de una placa del sistema fallida mediante la Clave base del sistema que está cifrada con una clave AES desbloqueada por la contraseña de Administrador de Client Security Solution o la frase de paso de Client Security.

A continuación, se crea la Clave hoja del sistema. Esta clave antigua se crea para proteger los secretos de nivel del sistema, ya que la clave EAS es utiliza por Rescue and Recovery para proteger las copias de seguridad.

Registrar usuario

Para que los datos de cada usuario estén protegidos mediante el mismo Módulo de plataforma fiable, cada usuario tendrá creada su propia Clave base de usuario. Esta clave de almacenamiento asimétrica que se puede migrar también se crea y protege dos veces mediante una clave AES simétrica generada a partir de cada contraseña de usuario de Windows o frase de paso de Client Security. La segunda instancia de la clave base de usuario se importa seguidamente en el Módulo de plataforma fiable y se protege mediante la SRK del sistema. Consulte Figura 2.

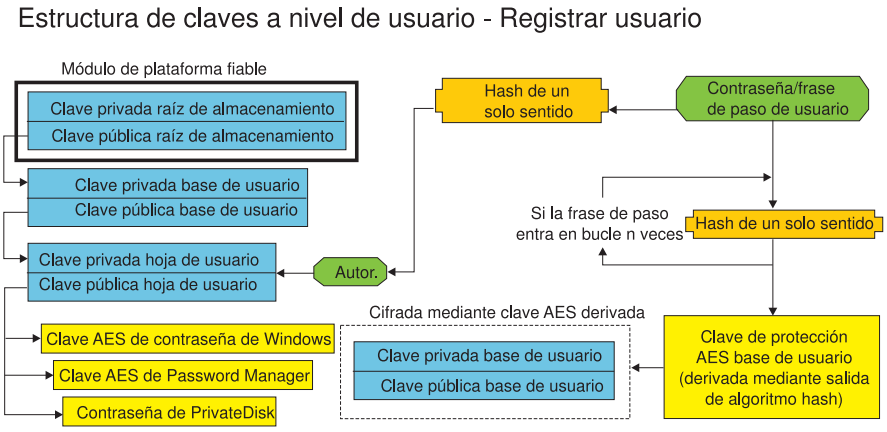

Figura 2.

Una vez que se haya creado la Clave base de usuario, se creará una clave asimétrica secundaria denominada Clave hoja de usuario a fin de proteger los secretos individuales como por ejemplo la clave AES de Password utilizada para proteger la información de inicio de sesión en Internet, la contraseña de PrivateDisk utilizada para proteger los datos y la clave AES de la contraseña de Windows utilizada para proteger el acceso al sistema operativo. El acceso a la Clave hoja de usuario lo controla la contraseña de Windows del usuario o la frase de paso de Client Security Solution y se desbloquea automáticamente durante el inicio de sesión.

Emulación de software

Si el sistema no tiene un Módulo de plataforma fiable, se utilizará una raíz de fiabilidad basada en software. La misma funcionalidad estará disponible al usuario, excepto que tendrá que disminuir la seguridad ya que la raíz de fiabilidad estará basada en claves basadas en software. La SRK del Módulo de plataforma fiable es sustituida por la clave RSA basada en software y la clave AES para proporcionar la protección que proporciona el Módulo de plataforma fiable. La clave RSA empaqueta la clave AES y la clave AES se utiliza para cifrar la siguiente clave RSA de la jerarquía.

Cambio de la placa del sistema

Un cambio de la placa del sistema implica que la SRK anterior a la que estaban vinculadas las claves ya no es válida, y es necesaria otra SRK. Esto también puede suceder si se borra mediante el BIOS el Módulo de plataforma fiable.

Es necesario que el administrador de Client Security Solution vincule las credenciales del sistema a una nueva SRK. Será necesario descifrar la Clave base

del sistema mediante la Clave de protección AES base del sistema derivada de las credenciales de autorización del administrador de Client Security Solution. Consulte Figura 3.

Nota: Si un administrador de Client Security Solution es un ID de usuario de dominio y la contraseña de dicho ID de usuario se ha cambiado en una máquina distinta, para descifrar la Clave base del sistema para la recuperación será necesario conocer la contraseña que se utilizó al iniciar sesión por última vez en el sistema. Por ejemplo, durante el despliegue se configurarán un ID de usuario y una contraseña de administrador de Client Security Solution; si la contraseña de este usuario cambia en una máquina distinta, la contraseña original establecida durante el despliegue será la autorización necesaria a fin de recuperar el sistema.

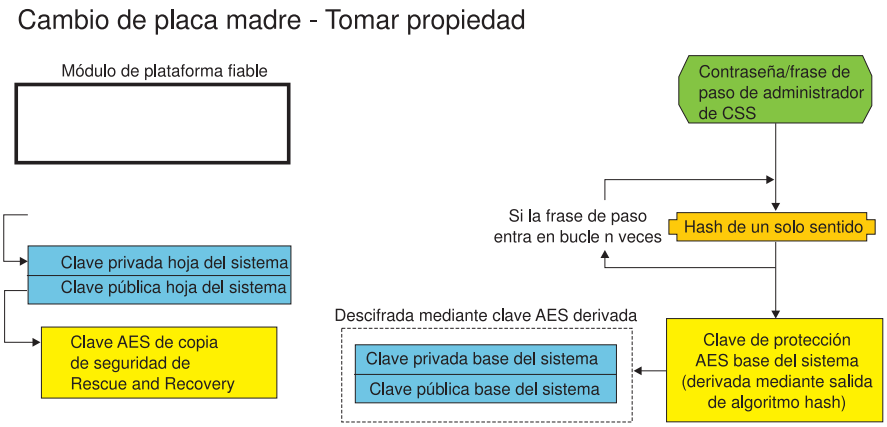

Figura 3.

Siga estos pasos para realizar un cambio de la placa del sistema:

1. El administrador de Client Security Solution inicia sesión en el sistema operativo.
2. El código ejecutado de inicio de sesión (cssplanarswap.exe) reconoce que el chip de seguridad está inhabilitado y requiere que se rearranque para habilitarlo. (Este paso se puede evitar habilitando el chip de seguridad mediante la BIOS.)
3. Se rearranca el sistema y se habilita el chip de seguridad.
4. El administrador de Client Security Solution inicia la sesión; finaliza el nuevo proceso de Tomar propiedad.
5. Se descifra la Clave base del sistema utilizando la Clave de protección AES base del sistema que se deriva de la autentificación de administrador de Client Security Solution. Se importa la Clave base del sistema en la nueva SRK y se restablece la Clave hoja del sistema y todas las credenciales protegidas por ésta.
6. El sistema está ahora recuperado.

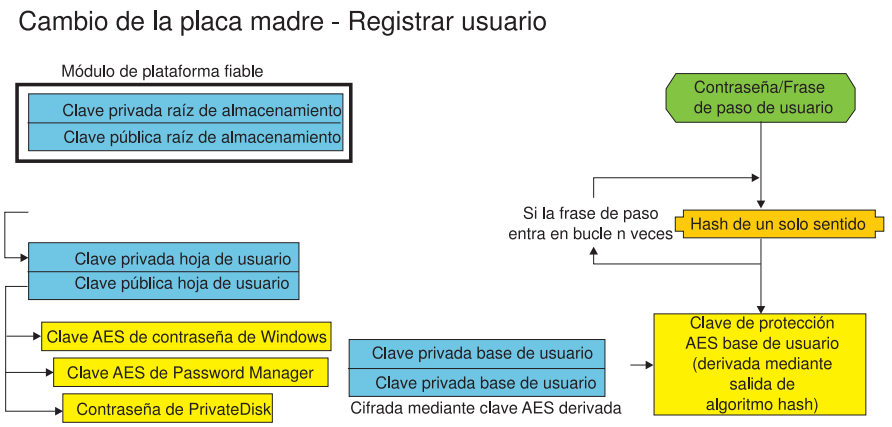

Figura 4.

Conforme cada usuario inicia sesión en el sistema, la Clave base de usuario se descifra automáticamente mediante la Clave de protección AES base de usuario derivada de la autentificación de usuario e importada a la nueva SRK creada mediante el administrador de Client Security Solution.

Esquema XML

El propósito de los scripts xml es permitir a los administrador de TI crear scripts personalizados que puedan utilizar para desplegar Client Security Solution. Todas las funciones que están disponibles en el Asistente de configuración de Client Security Solution están también disponibles mediante los scripts. Los scripts se pueden proteger mediante el ejecutable xml_crypt_tool (con una contraseña (cifrado AES) o una ocultación). Una vez creada, la máquina virtual (vmserver.exe) acepta los scripts como entrada. La máquina virtual llama a las mismas funciones que el Asistente de configuración para configurar el software.

Uso

Todos los scripts constan de una etiqueta para especificar el tipo de codificación xml, el esquema xml, y como mínimo de una función a realizar. El esquema se utiliza para validar el archivo xml y comprobar si existen los parámetros necesarios. Actualmente no se fuerza la utilización del esquema. Cada función está entre etiquetas de función. Cada función contiene una orden que especifica el orden en el que la máquina virtual (vmserver.exe) ejecutará el mandato. Cada versión tiene también un número de versión; actualmente todas las funciones están en la versión 1.0. Con el propósito de que sean más claros, cada uno de los siguientes scripts de ejemplo sólo contiene una función. Sin embargo, en la práctica un script contendrá posiblemente varias funciones. El Asistente de configuración de Client Security Solutions se puede utilizar para crear un script de este tipo. Consulte “Asistente de Client Security” en la página 167 (consulte la documentación del asistente de configuración para obtener información más detallada).

Nota: Si se omite el parámetro <DOMAIN_NAME_PARAMETER> en cualquiera de las funciones que requiere un nombre de dominio, se utilizará el nombre del sistema por omisión.

Ejemplos

AUTO_ENROLL_ADMIN_FOR_RNR_ONLY

Este mandato permite al administrador del sistema generar las claves de seguridad necesarias para cifrar las copias de seguridad con Rescue and Recovery. Este mandato se debe ejecutar sólo una vez por cada sistema; no debe debe ejecutar para cada usuario, sólo el administrador.

Nota: Para instalaciones de sólo Rescue and Recovery, se debe asignar un administrador como el propietario del TPM si se van a cifrar copias de seguridad con el TPM. Utilice el siguiente archivo script para asignar automáticamente un ID de usuario y una contraseña de administrador. Este ID de usuario y contraseña de Windows se utilizarán para la recuperación del TPM. (Ninguna de las demás funciones de script XML de CSS es aplicable si sólo está instalado Rescue and Recovery.)

- **USER_NAME_PARAMETER**

  ID de usuario de Windows del usuario administrador.
- **DOMAIN_NAME_PARAMETER**

  Nombre de dominio del usuario administrador.
- **RNR_ONLY_PASSWORD**

  Contraseña de Windows del usuario administrador.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>AUTO_ENROLL_ADMIN_FOR_RNR_ONLY</COMMAND>
          <VERSION>1.0</VERSION>
          <USER_NAME_PARAMETER>NombreAdminWin</USER_NAME_PARAMETER
          <DOMAIN_NAME_PARAMETER>MiEmpr</DOMAIN_NAME_PARAMETER>
          <RNR_ONLY_PASSWORD>C0ntraseñaWin<RNR_ONLY_PASSWORD>
         </FUNCTION>
</CSSFile>
```

ENABLE_TPM_FUNCTION

Este mandato habilita el Módulo de plataforma fiable y utiliza el argumento SYSTEM_PAP. Si el sistema ya tiene establecida una contraseña de administrador/supervisor del BIOS, no se proporcionará este argumento. De lo contrario, este mandato es opcional.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>ENABLE_TPM_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
          <SYSTEM_PAP>PASSWORD</SYSTEM_PAP>
         </FUNCTION>
</CSSFile>
```

DISABLE_TPM_FUNCTION

Este mandato utiliza el argumento SYSTEM_PAP. Si el sistema ya tiene establecida una contraseña de administrador/supervisor del BIOS, no se proporcionará este argumento. De lo contrario, este mandato es opcional.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>DISABLE_TPM_FUNCTION</COMMAND>
```

```
          <VERSION>1.0</VERSION>
          <SYSTEM_PAP>contraseña</SYSTEM_PAP>
         </FUNCTION>
</CSSFile>
```

ENABLE_ENCRYPT_BACKUPS_FUNCTION

Cuando utiliza Rescue and Recovery, este mandato habilita la protección de las copias de seguridad con Client Security Solution.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>ENABLE_ENCRYPT_BACKUPS_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

DISABLE_ENCRYPT_BACKUPS_FUNCTION

Al utilizar Rescue and Recovery para proteger las copias de seguridad, este mandato inhabilita la protección de las copias de seguridad con Client Security Solution.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>DISABLE_ENCRYPT_BACKUPS_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENABLE_PWMGR_FUNCTION

Este mandato habilita Password Manager para todos los usuarios de Client Security Solution.

```
 <?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>ENABLE_PWMGR_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENABLE_CSS_GINA_FUNCTION

Este mandato habilita el Inicio de sesión de Client Security Solution.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>ENABLE_CSS_GINA_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENABLE_UPEK_GINA_FUNCTION

Si está instalado el Software de huellas dactilares de ThinkVantage, este mandato habilita el Inicio de sesión.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
```

```
          <COMMAND>ENABLE_UPEK_GINA_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENABLE_UPEK_GINA_WITH_FUS_FUNCTION

Si está instalado el Software de huellas dactilares de ThinkVantage, este mandato habilita el soporte de Iniciar sesión con el cambio rápido de usuario.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>ENABLE_UPEK_GINA_WIH_FUS_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENABLE_NONE_GINA_FUNCTION

Si el Software de huellas dactilares de ThinkVantage o el Inicio de sesión de Client Security Solution está habilitado, este mandato inhabilita los Inicios de sesión del Software de huellas dactilares de ThinkVantage y de Client Security Solution.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>ENABLE_CSS_NONE_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

SET_PP_FLAG_FUNCTION

Este mandato graba un distintivo que Client Security Solution lee para determinar si se debe utilizar la frase de paso de Client Security o una contraseña de Windows.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>SET_PP_FLAG_FUNCTION</COMMAND>
         <PP_FLAG_SETTING_PARAMETER>USE_CSS_PP</PP_FLAG_SETTING_PARAMETER>
         <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENABLE_PRIVATEDISK_PROTECTION_FUNCTION

Este mandato permite que se utilice SafeGuard PrivateDisk en el sistema. De todas formas, se debe configurar cada usuario específicamente para utilizar Safeguard PrivateDisk mediante ENABLE_PD_USER_FUNCTION.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>ENABLE_PRIVATEDISK_PROTECTION_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

SET_ADMIN_USER_FUNCTION

Este mandato graba un distintivo que Client Security Solution lee para determinar quién es el usuario administrador de Client Security Solution. Los parámetros son:

- **USER_NAME_PARAMETER**

  Nombre de usuario del usuario administrador.
- **DOMAIN_NAME_PARAMETER**

  Nombre de dominio del usuario administrador.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>SET_ADMIN_USER_FUNCTION</COMMAND>
          <USER_NAME_PARAMETER>sabedi</USER_NAME_PARAMETER>
          <DOMAIN_NAME_PARAMETER>IBM-2AA92582C79<DOMAIN_NAME_PARAMETER>
          <VERSION>1.0</VERSION>
          <SYSTEM_PAP>PASSWORD</SYSTEM_PAP>
         </FUNCTION>
</CSSFile>
```

ENABLE_PD_USER_FUNCTION

Este mandato permite a un usuario determinado utilizar PrivateDisk. Los parámetros son los siguientes:

- **USER_NAME_PARAMETER**

  Nombre de usuario del usuario para habilitar PrivateDisk.
- **DOMAIN_NAME_PARAMETER**

  Nombre de dominio del usuario para habilitar PrivateDisk.
- **PD_VOLUME_SIZE_PARAMETER**

  Tamaño del volumen PrivateDisk en megabytes.
- **PD_VOLUME_PATH_PARAMETER**

  Vía de acceso del volumen PrivateDisk que se creará.
- **PD_VOLUME_NAME_PARAMETER**

  Nombre del volumen PrivateDisk que se creará. Si se especifica el valor PD_USE_DEFAULT_OPTION, se utilizará automáticamente el valor por omisión.
- **PD_VOLUME_DRIVE_LETTER_PARAMETER**

  Letra de la unidad del volumen PrivateDisk que se creará. Si se especifica el valor PD_USE_DEFAULT_OPTION, se utilizará automáticamente un valor por omisión.
- **PD_VOLUME_CERT_PARAMETER**

  Si se pasa el valor PD_USE_CSS_CERT, PrivateDisk creará un nuevo certificado o utilizará un certificado existente y lo protegerá mediante CSP de Client Security Solution. El montaje/desmontaje de este volumen estará ligado al CSP en lugar de estarlo a la frase de paso de CSS/contraseña de Windows. Si se especifica el valor PD_USE_DEFAULT_OPTION, no se utilizará ningún certificado y se adoptará el valor por omisión de la frase de paso de CSS/contraseña de Windows del usuario.
- **PD_USER_PASSWORD**

  Contraseña que Client Security Solution pasa a PrivateDisk para montar/crear el volumen PrivateDisk. Si se especifica el valor PD_RANDOM_VOLUME_PWD, Client Security Solution generará una contraseña aleatoria del volumen.
- **PD_VOLUME_USER_PASSWORD_PARAMETER**

  Contraseña específica del usuario para montar el volumen PrivateDisk. La finalidad de esta contraseña es ser una copia de seguridad de la contraseña PD_USER_PASSWORD. Si, por alguna razón, Client Security Solution falla en el

futuro, el valor pasado a este argumento será independientemente de Client Security Solution. Si se especifica el valor PD_USE_DEFAULT_OPTION, no se utilizará ningún valor.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>ENABLE_PD_USER_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
          <USER_NAME_PARAMETER>sabedi</USER_NAME_PARAMETER>
          <DOMAIN_NAME_PARAMETER>IBM-2AA92582C79<DOMAIN_NAME_PARAMETER>
          <PD_VOLUME_SIZE_PARAMETER>500</PD_VOLUME_SIZE_PARAMETER>
          <PD_VOLUME_PATH_PARAMETER>C:\Documents and Settings\sabedi\My Documents\
             </PD_VOLUME_PATH_PARAMETER>
          <PD_VOLUME_NAME_PARAMETER>PD_USE_DEFAULT_OPTION</PD_VOLUME_NAME_PARAMETER>
          <PD_VOLUME_DRIVE_LETTER_PARAMETER>PD_USE_DEFAULT_OPTION</PD_VOLUME_DRIVE
             _LETTER_PARAMETER>
          <PD_VOLUME_CERT_PARAMETER>PD_USE_DEFAULT_OPTION</PD_VOLUME_CERT_PARAMETER>
          <PD_VOLUME_USER_PASSWORD_PARAMETER>PD_USE_DEFAULT_OPTION</PD_VOLUME_
             USER_PASSWORD_
             PARAMETER>
          <PD_USER_PASSWORD>PD_RANDOM_VOLUME_PWD</PD_USER_PASSWORD>
         </FUNCTION>
</CSSFile>
```

INITIALIZE_SYSTEM_FUNCTION

Este mandato inicializa el sistema en Client Security Solution para ser utilizado en el sistema. Todas las claves amplias del sistema se generan mediante esta llamada de función. Los parámetros son los siguientes:

- **NEW_OWNER_AUTH_DATA_PARAMETER**

  La contraseña del propietario inicializa el sistema. Si no se establece la contraseña de propietario, el valor pasado para este argumento se convertirá en la nueva contraseña de propietario. Si ya está establecida una frase de paso de propietario y el administrador utiliza la misma contraseña, se podrá pasar. En el caso de que el administrador desee utilizar una nueva frase de paso de propietario, se deberá pasar la contraseña que se desee en este parámetro.

- **CURRENT_OWNER_AUTH_DATA_PARAMETER**

  Contraseña del propietario actual del sistema. Si el sistema ya tiene una contraseña de propietario 5.4x, este parámetro se debe pasar en la contraseña 5.4x. De lo contrario, si se desea una nueva contraseña de propietario, se debe pasar la contraseña de propietario actual en este parámetro. Si no se desea realizar ningún cambio de contraseña, se debe pasar el valor NO_CURRENT_OWNER_AUTH.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>INITIALIZE_SYSTEM_FUNCTION</COMMAND>
          <NEW_OWNER_AUTH_DATA_PARAMETER>contra1seña</NEW_OWNER_AUTH_DATA_
              PARAMETER>
          <CURRENT_OWNER_AUTH_DATA_PARAMETER>No_CURRENT_OWNER_AUTH</CURRENT
              _OWNER_AUTH_DATA_PARAMETER>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

CHANGE_TPM_OWNER_AUTH_FUNCTION

Este mandato cambia la autorización de administrador de Client Security Solution y actualiza las claves del sistema en consecuencia. Todas las claves amplias del sistema se generan mediante esta llamada de función. Los parámetros son los siguientes:

- NEW_OWNER_AUTH_DATA_PARAMETER

  Nueva contraseña de propietario del Módulo de plataforma fiable.
- CURRENT_OWNER_AUTH_DATA_PARAMETER

  Contraseña de propietario actual del Módulo de plataforma fiable.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>CHANGE_TPM_OWNER_AUTH_FUNCTION</COMMAND>
          <NEW_OWNER_AUTH_DATA_PARAMETER>nuevaContraseña</NEW_OWNER_AUTH_DATA_
              PARAMETER>
          <CURRENT_OWNER_AUTH_DATA_PARAMETER>ContraseñaAntigua</CURRENT_OWNER_AUTH
              _DATA_PARAMETER>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENROLL_USER_FUNCTION

Este mandato registra un usuario determinado para utilizar Client Security Solution. Esta función crea todas las claves de seguridad específicas del usuario para un usuario determinado. Los parámetros son los siguientes:

- **USER_NAME_PARAMETER**

  Nombre de usuario del usuario que se registrará.
- **DOMAIN_NAME_PARAMETER**

  Nombre de dominio del usuario que se registrará.
- **USER_AUTH_DATA_PARAMETER**

  Contraseña del Módulo de plataforma fiable/contraseña de Windows con la que se crearán las claves de seguridad del usuario.
- **WIN_PW_PARAMETER**

  Contraseña de Windows.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>ENROLL_USER_FUNCTION</COMMAND>
          <USER_NAME_PARAMETER>sabedi</USER_NAME_PARAMETER>
          <DOMAIN_NAME_PARAMETER>IBM-2AA92582C79<DOMAIN_NAME_PARAMETER>
          <USER_AUTH_DATA_PARAMETER>miFrasepasoUsuarioCss</USER_AUTH_DATA_PARAMETER>

          <WIN_PW_PARAMETER>miContraseñaWindows</WIN_PW_PARAMETER>
          <VERSION>1.0</VERSION>
          </FUNCTION>
</CSSFile>
```

USER_PW_RECOVERY_FUNCTION

Este mandato establece una recuperación de contraseña de un usuario determinado del Módulo de plataforma fiable. Los parámetros son los siguientes:

- **USER_NAME_PARAMETER**

  Nombre de usuario del usuario que se registrará.
- **DOMAIN_NAME_PARAMETER**

Nombre de dominio del usuario que se registrará.

- **USER_PW_REC_QUESTION_COUNT**

  Número de preguntas que el usuario debe responder.

- **USER_PW_REC_ANSWER_DATA_PARAMETER**

  Respuesta almacenada a una pregunta determinada. Tenga en cuenta que el nombre real de este parámetro está concadenado con un número que se corresponde con la pregunta a la que responde. Consulte el ejemplo de este mandato que se muestra a continuación.

- **USER_PW_REC_STORED_PASSWORD_PARAMETER**

  Contraseña almacenada que se presenta al usuario una vez que se han contestado correctamente todas las preguntas.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>USER_PW_RECOVERY_FUNCTION</COMMAND>
          <USER_NAME_PARAMETER>sabedi</USER_NAME_PARAMETER>
          <DOMAIN_NAME_PARAMETER>IBM-2AA92582C79<DOMAIN_NAME_PARAMETER>
          <USER_PW_REC_ANSWER_DATA_PARAMETER>Prueba1</USER_PW_REC_ANSWER_DATA_
              PARAMETER>
          <USER_PW_REC_ANSWER_DATA_PARAMETER>Prueba2</USER_PW_REC_ANSWER_DATA_
              PARAMETER>
          <USER_PW_REC_ANSWER_DATA_PARAMETER>Prueba3</USER_PW_REC_ANSWER_DATA_
              PARAMETER>
          <USER_PW_REC_QUESTION_COUNT>3</USER_PW_REC_QUESTION_COUNT>
          <USER_PW_REC_QUESTION_LIST>20000,20001,20002</USER_PW_REC_QUESTION_LIST>
         </USER_PW_REC_STORED_PASSWORD_PARAMETER>Contra1seña</USER_PW_REC_
              STORED_PASSWORD_PARAMETER>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

SET_WIN_PE_LOGON_MODE_FUNCTION

Este mandato graba un distintivo que el programa lee para determinar si es necesaria la autorización de usuario al entrar en el entorno de Windows PE. El parámetro es el siguiente:

- **WIN_PE_LOGON_MODE_AUTH_PARAMETER**

  Las dos opciones válidas son:

  – NO_AUTH_REQUIRED_FOR_WIN_PE_LOGON

  – AUTH_REQUIRED_FOR_WIN_PE_LOGON

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
         <FUNCTION>
          <ORDER>0001</ORDER
          <COMMAND>SET_WIN_PE_LOGON_MODE_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
          <WIN_PE_LOGON_MODE_AUTH_PARAMETER>AUTH_REQUIRED_FOR_WIN_PE_LOGON</WIN
             _PE_LOGON_MODE_AUTH_PARAMETER>
          <SYSTEM_PAP>PASSWORD</SYSTEM_PAP>
         </FUNCTION>
</CSSFile>
```

Capítulo 5. Personalización de System Migration Assistant

Hay dos partes de System Migration Assistant personalizables:

- Edicion o modificación de un archivo de mandatos
- Migración de valores de aplicaciones adicionales

Creación de un archivo de mandatos

Durante la fase de captura, SMA lee el contenido del archivo de mandatos y los valores de archivado. Esta sección contiene información acerca de los archivos de mandatos y las sentencias que pueden contener.

System Migration Assistant proporciona un archivo de mandatos por omisión (command.xml) que puede utilizar como plantilla para crear un archivo de mandatos personalizado. Si ha instalado SMA en la ubicación por omisión, este archivo está ubicado en el directorio D:\%RR%\migration\bin.

Nota: System Migration Assistant 5.0 utiliza tecnología XML para describir sus mandatos del archivo de mandatos.

Tenga en cuenta los puntos siguientes en relación de los archivos de mandatos de SMA 5.0:

- El archivo de mandatos sigue la sintaxis de XML versión 1.0 y el archivo de mandatos es sensible a mayúsculas y minúsculas.
- Cada sección de mandato y parámetro se debe iniciar con <TagName> y finalizar con </TagName>, y su valor se debe escribir entre esas etiquetas.
- Los errores de sintaxis pueden causar un error al ejecutar SMA. Si SMA encuentra un error, graba el error en el archivo de registro y continúa la operación. En función de la gravedad del error, es posible que los resultados finales sean defectuosos.

Mandatos del archivo de mandatos

La tabla siguiente contiene información acerca de los mandatos, con la excepción de aquellos que hacen referencia a la migración de archivos o al registro, que se pueden utilizar en un archivo de mandatos:

Tabla 10.

Mandato	Parámetros	Valores de los parámetros y ejemplos

<Desktop>	• <accessability>
	• <active_desktop>
	• <colors>
	• <desktop_icons>
	• <display>
	• <icon_metrics>
	• <keyboard>
	• <mouse>
	• <pattern>
	• <screen_saver>
	• <sento_menu>
	• <shell>
	• <sound>
	• <start_menu>
	• <taskbar>
	• <wallpaper>
	• <window_metrics>
		Para seleccionar un valor del escritorio, establezca el parámetro en "true". De lo contrario, establezca el parámetro en "false" o déjelo sin especificar.
		
		Por ejemplo:
		`<Desktop>`
		`<colors>true</colors>`
		`<desktop_icons>true</desktop_icons>`
		`<screen_saver>true</screen_saver>`
		`<start_menu>false</start_menu>`
		`<time_zone>true</time_zone>`
		`</Desktop>`

<Network>	• <ip_subnet_gateway_configuration>
	• <dns_configuration>
	• <wins_configuration>
	• <computer_name>
	• <computer_description>
	• <domain_workgroup>
	• <mapped_drives>
	• <shared_folders_drives>
	• <dialup_networking>
	• <odbc_datasources>
		Para seleccionar un valor del escritorio, establezca el parámetro en "true". De lo contrario, establezca el parámetro en "false" o déjelo sin especificar.
		
		Por ejemplo:
		`<Network>`
		`<computer_name>true<computer_name>`
		`<mapped_drives>false</mapped_drives>`
		`</Network>`

<Applications>	<Application>
	
	Consulte el manual *ThinkVantage System Migration Assistant Guía del usuario* para ver una lista de todas las aplicaciones a las que se da soporte.
		Por ejemplo:
		`<Applications>`
		`<Application>Lotus Notes</Application>`
		`<Application>Microsoft Office</Application>`
		`<//Applications>`
		
		o bien
		`<Applications>`
		`<Application>$(all)</Applications>`

<Registries>	• <Registry> • <hive> • <keyname> • <value>	Para capturar o aplicar los valores del registro, especifique hive, keyname y value como los parámetros del archivo de mandatos.

Tabla 10. (continuación)

Mandato	Parámetros	Valores de los parámetros y ejemplos

<IncUsers>	<UserName>	Para capturar todos los perfiles de usuario, establezca $(all) o utilice * como carácter comodín para todos los usuarios. De lo contrario, especifique los usuarios individualmente.
		
		Están disponibles los siguientes caracteres comodín.
		• * para un carácter comodín de longitud variable
		• % para un carácter comodín de longitud fija (1 carácter)
		
		For ejemplo:
		`<IncUsers>`
		`<UserName>administrator</UserName>`
		`<UserName>domain\Jim</UserName>`
		`</IncUsers>`

<ExcUsers>	<UserName>	Para excluir usuarios del proceso de migración, especifique el dominio y el nombre de usuario del usuario. Están disponibles los siguientes caracteres comodín. • * para un carácter comodín de longitud variable • % para un carácter comodín de longitud fija (1 carácter)

<Printers>	<Printer>
	
	<PrinterName>
		Esta sentencia de control es efectiva tanto para el sistema origen como para el sistema destino.
		
		Para capturar todas las impresoras, establezca el parámetro en *&(all)*. De lo contrario, especifique cada impresora individualmente. Para capturar solamente la impresora por omisión, establezca el parámetro en *&(DefaultPrinter)*.
		
		For ejemplo:
		`<Printers>`
		`  <Printer>&(all)</Printer>`
		`</Printers>`
		
		`<Printers>`
		`  <Printer>`
		`  <PrinterName>IBM 5589-L36</PrinterName>`
		`  </Printer>`
		`</Printers>`
		
		`<Printers>`
		`  <Printer>&(DefaultPrinter)</Printer>`
		`</Printers>`

Tabla 10. (continuación)

Mandato	Parámetros	Valores de los parámetros y ejemplos
<MISC>	<bypass_registry>	Para deseleccionar todos los valores del registro, establézcalo en “true”. De lo contrario, establézcalo en “false” o déjelo sin especificar.
	<overwrite existing files>	Para sobregrabar archivos existentes, establézcalo en “true”. De lo contrario, establézcalo en “alse” o déjelo sin especificar.
	<log_file_location>	Para especificar el directorio en el que SMA graba los archivos de registro, especifique un nombre de directorio totalmente calificado. Puede especificar un directorio compartido en otro sistema. Si no establece este parámetro, SMA graba los archivos de registro en d:/DirInst/, donde d es la letra de la unidad de disco duro y /DirInst/ es el directorio donde está instalado SMA.
	<temp_file_location>	Para especificar el directorio en el que SMA graba los archivos temporales, entre un nombre de directorio totalmente calificado. Puede especificar un directorio compartido en otro sistema. Si no establece este parámetro, SMA graba los archivos temporales en d:/DirInst/etc/data, donde d es la letra de la unidad de disco duro y /DirInst/ es el directorio donde está instalado SMA.
	<resolve_icon_links>	Para copiar sólo aquellos iconos que tienen enlaces activos, establézcalo en “true”. De lo contrario, establezca el parámetro en “false” o déjelo sin especificar.

Mandatos de migración de archivos

SMA procesa los mandatos de migración de archivos en el orden siguiente: primero se realizan los mandatos de inclusión de archivos y, a continuación, se realizan los mandatos de exclusión de archivos para los archivos de inclusión.

SMA seleccionará y deseleccionará los archivos según la ubicación original de archivos y carpetas en el sistema origen. Las sentencias de redireccionamiento de archivos se almacenan en el perfil y se interpretan durante la fase de aplicación.

El proceso de los nombres de archivos y directorios no es sensible a mayúsculas y minúsculas.

La tabla siguiente contiene información acerca de los mandatos de migración de archivos. Todos los mandatos de migración de archivos son opcionales.

Tabla 11.

Mandato	Parámetro	Qué hace

<FilesAndFolders>	<run>	Para capturar o aplicar la migración de archivos, establezca el parámetro en “true”. De lo contrario, establezca el parámetro en “false” o déjelo sin especificar.
		
		For ejemplo:
		
		`<FilesAndFolders>`
		`<run>true</run>`
		`</FilesAndFolders>`

<Exclude_drives>	<Drive>	Especifique la letra de la unidad para excluir unidades de la exploración.
		
		For ejemplo:
		
		`<ExcludeDrives>`
		`<Drive>D</Drive>`
		`<Drive>E</Drive>`
		`</ExcludeDrive>`

Tabla 11. (continuación)

Mandato	Parámetro	Qué hace

<Inclusions>	<IncDescriptions>
	<Description>
	<DateCompare>
	<Operand>
	<Date>
	<SizeCompare>
	<Operand>
	<Size>
	<Dest>
	<Operation> donde
	• <Description> es el nombre del archivo totalmente calificado. Puede utilizar un carácter comodín tanto para el nombre de archivo como para el nombre de carpeta.
	• <DateCompare> es un parámetro opcional que especifica los archivos según la fecha en la que se crearon.
	– <Operand> es NEWER u OLDER.
	– <Date> es la fecha de línea base en el formato mm/dd/aaaa.
	• <SizeCompare> es un parámetro opcional para seleccionar archivos en base a su tamaño.
	– <Operand> es LARGER o SMALLER.
	– <Size> es el tamaño del archivo en MB.
	• <Dest> es un parámetro opcional que especifica el nombre de la carpeta de destino en el sistema destino donde se grabarán los archivos.
	• <Operation> es un parámetro opcional que especifica cómo se manejará la vía de acceso de los archivos. Especifique una de las opciones siguientes:
	– P conserva la vía de acceso del archivo y vuelve a crear el archivo en el sistema destino empezando en la ubicación especificada por el parámetro <Dest>.
	– R elimina la vía de acceso del archivo y cola el archivo directamente en la ubicación especificada por el parámetro <Dest>.
		Busca todos los archivos coincidentes en los directorios especificados.
		Por ejemplo:
		Ejemplo 1
		`<IncDescription>`
		`<Description>c:\MiCarpetaTrabajo\ls</Description>`
		`</IncDescription>`
		Nota: Nota: Para especificar el nombre de la carpeta, añada .\. al final de la descripción
		Ejemplo 2
		`<IncDescription>`
		`<Description>C:\MiCarpetaTrabajo\*.*</Decsription>`
		`<DateCompare>`
		`<Operand>NEWER</Operand>`
		`<Date>07/31/2005</Date>`
		`</DateCompare>`
		`</IncDescription>`
		Ejemplo 3
		`<IncDescription>`
		`<Description>C:\MiCarpetaTrabajo/*.*</Description>`
		`<SizeCompare>`
		`<Operand>SMALLER</Operand>`
		`<Size>200</Size>`
		`</SizeCompare>`
		`</IncDescription>`
		Ejemplo 4
		`<IncDescription>`
		`<Description>C:\MiCarpetaTrabajo\*.*</Description>`
		`<Dest>D:\MiNuevaCarpetaTrabajo</Dest>`
		`<Operation>`
		`<IncDescription>`

Tabla 11. (continuación)

Mandato	Parámetro	Qué hace

<Exclusions>	<ExDescriptions>
	<Description>
	<DateCompare>
	<Operand>
	<Date>
	<SizeCompare>
	<Operand>
	<Size> donde
	• <Description> es un nombre de archivo o un nombre de carpeta totalmente calificado. Puede contener caracteres comodín tanto para el nombre del archivo como para el nombre de la carpeta.
	• DateCompare> es un mandato opcional que puede utilizar para seleccionar archivos según la fecha en la que se crearon.
	– <Operand> es NEWER o OLDER.
	– <Date> es la fecha de línea base en el formato mm/dd/aaaa.
	• <SizeCompare> es un parámetro opcional para seleccionar archivos en base a su tamaño.
	– <Operand> es LARGER o SMALLER.
	– <Size> es el tamaño del archivo en MB.
		Deselecciona todos los archivos coincidentes en un directorio especificado
		Por ejemplo:
		Ejemplo 1
		`<ExDescription>`
		`<Description>C:\MiCarpetaTrabajo</Description>`
		`</ExDescription>`
		Ejemplo 2
		`<ExDescription>`
		`<Description>C:\MiCarpetaTrabajo</Desccription>`
		`<DateCompare>`
		`<Operand>OLDER</Operand>`
		`<Date>07/31/2005</Date>`
		`</DateCompare>`
		`</ExDescription>`
		Ejemplo 3
		`<ExDescription>`
		`<Description>C:\MiCarpetaTrabajo</Description>`
		`<SizeCompare>`
		`<Operand>LARGER</Operand>`
		`<Size>200</Size></SizeCompare>`
		`</ExDescription>`

Ejemplos de mandatos de migración de archivos

Esta sección contiene ejemplos de mandatos de migración de archivos. Estos ejemplos demuestran cómo combinar los mandatos de inclusión de archivos y de exclusión de archivos para refinar la selección de archivos. Sólo se muestran las secciones de manejo de archivos del mandato.

Selección de archivos durante la fase de captura

Esta sección contiene tres ejemplos de código utilizado para seleccionar archivos durante la fase de captura.

Ejemplo 1

El ejemplo de código siguiente selecciona todos los archivos con una extensión .doc (documentos de Microsoft) y los vuelve a colocar en el directorio “d:\Mis Documentos”. A continuación, excluye todos los archivos que están en el directorio d:\Ya_No_Utilizados

```
<IncDescription>
<Description>*:\*.doc/s</Description>
<Dest>d:\Mis Documentos</Dest>
<Operation>r</Operation>
<IncDescription>
</Inclusions>
<Exclusions>
<ExcDescription>
<Description>d:\Ya_No_Utilizados\</Description>
</ExcDescription>
</Exclusions>
```

Ejemplo 2

El siguiente ejemplo de código selecciona el contenido de la unidad, excluyendo todos los archivos ubicados en la raíz de la unidad d y todos los archivos con una extensión .tmp.

```
<Inclusions>
<IncDescription>
<Description<d:\*.*/s<\Description>
</IncDescription>
</Inclusions>
<Exclusions>
<ExcDescription>
<Description>d:\*.*</Description>
</ExcDescription>
<ExcDescription>
<Description>*:\*.tmp/s</Description>
</ExcDescription>
</Exclusions>
```

Ejemplo 3

: El ejemplo de código siguiente selecciona todo el contenido de la unidad c, excluyendo todos los archivos ubicados en %windir% que especifica el directorio de Windows.

```
<Inclusions>
<IncDescription>C:\*.*/s</Description>
</Inclusion>
<Exclusions>
<ExcDescription>
<Description>%windir%\</Description>
</ExcDescription>
</Exclusions>
```

Ejemplo 4

El siguiente ejemplo de código selecciona todo el contenido de la carpeta %PERFILUSUARIO% que es la vía de acceso del Perfil de usuario del usuario que ha iniciado la sesión actualmente, excluyendo todos los archivos con una extensión .dat y la subcarpeta “Local Settings”.

```
<Inclusions>
<IncDescription>
<Description>%PERFILUSUARIO%\</Description>
</IncDescription>
</Inclusions>
<Exclusions>
```

Migración de valores de aplicaciones adicionales

Nota: Para crear archivos de aplicaciones personalizados, debe tener un gran conocimiento de la aplicación, incluidas las ubicaciones de almacenamiento de los valores personalizados. Por omisión, SMA está preconfigurado para migrar valores para varias aplicaciones. Para ver una lista de las aplicaciones a las que SMA da

soporte, consulte el manual *System Migration Assistant Guía del usuario*. También puede crear un archivo de aplicación personalizado para migrar valores para aplicaciones adicionales.

Este archivo deben recibir el nombre aplicación.xml o aplicación.smaapp y estar ubicado en d:\%RR%\Migration\bin\Apps, donde *Apps* especifica la aplicación y d es la letra de la unidad de disco duro. Se da prioridad a aplicación.smaapp cuando existen los dos archivos de aplicaciones personalizadas de la misma aplicación, aplicación.smaapp y aplicación.xml.

Para dar soporte a una nueva aplicación, puede copiar un archivo de aplicación existente y realizar los cambios necesarios. Por ejemplo, Microsoft_Access.xml es un archivo de aplicación existente.

Tenga en cuenta los puntos siguientes acera de los archivos de aplicación:

- *aplicación*.xml
  - Por omisión, cuando se instala System Migration Assistant, sólo existe aplicación.xml.
  - La <etiqueta> que está entre "<!-" y "->" se trata como comentario. Por ejemplo:

    ```
    <!--Files_From_Folders>
    <!-Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi\*.* /s
    <Files_From_Folder>
     <Files_From_Folder>%Personal Directory%\*.pdf</Files_from_Folder>
    </Files_From_folders-->
    ```

  - Cada mandato se debe describir en una sección distinta.
  - Cada sección empieza con un mandato entre etiquetas, por ejemplo <AppInfo> o <Install_Directories>. Puede entrar uno o más campos en una sección; cada campo debe estar en una línea distinta.
  - Si el archivo de aplicación contiene errores de sintaxis, SMA continúa la operación y graba los errores en el archivo de registro

La Tabla 12 en la página 68 muestra información sobre los archivos de aplicación:

Tabla 12.

Sección	Mandato	Valor	Qué hace
<Applications>			
	<Family>	Una serie de texto. Los espacios que la preceden se ignoran; no coloque la serie de texto entre comillas.	Especifica el nombre no específico de versión de la aplicación. Cuando se ejecuta SMA en modalidad de proceso por lotes, el usuario utiliza esta serie de texto en la sección de las aplicaciones del archivo de mandatos. Por ejemplo: `<Family>adobe Acrobat Reader</Family>`
	<SMA_Version>	Un valor numérico	Especifica el número de versión de SMA. Por ejemplo, `<SMA_Version>SMA 5.0</SMA_Version`
	<App>	*NombreCorto* donde NombreCorto es un nombre corto específico de la versión para una aplicación.	Especifica un nombre corto específico de la versión para una o más aplicaciones. Por ejemplo, `<APP>Acrobat_Reader_50</APP>`
<Application ShortName=*NombreCorto*> donde *NombreCorto* es el nombre corto de una aplicación que ha especificado en la sección “Applications”.			
	<Name>	Una serie de texto	Especifica el nombre de la aplicación
	<Version>	Un valor numérico	Especifica la versión de la aplicación.

	<Detects>
	
	<Detect>
		Root, PathAndKey	Especifica una clave de registro. SMA detecta una aplicación buscando la clave de registro especificada.
			
			Por ejemplo,
			`<Detects>`
			`<Detect>`
			`<hive>HKLM</hive>`
			`<keyname>Software\Adobe\Acrobat Reader\5.0\</keyname>`
			`</Detect>`
			`</Detects>`

<Install_Directories>
 	
Por ejemplo:
`<Install_Directories>`
`<Install_Directory>`
`<OS>WinXP</OS>`
`<Registry>`
`<hive>HKLM</hive>`
`<keyname>Software\Adobe\Acrobat Reader\5.0\InstallPath</keyname>`
`<value>(Default)</value>`
`</Registry>`
`</Install_Directory>`
`<Install_Directory>`
`<OS>Win2000</OS>`
`<Registry>`
`<hive>HKLM</hive>`
`<keyname>Software\adobe\Acrobat Reader\5.0\InstallPath</keyname>`
`<value>(Default)</value>`
`</Registry>`
`</Install_Directory>`
`</Install_Directories>`			

Tabla 12. (continuación)

Sección	Mandato	Valor	Qué hace
	<OS>	Una serie de texto	OS especifica el sistema operativo y puede ser uno de los siguientes: • WinXP • Win2000 • WinNT • Win98
	<Registry>	*hive* es HKLM o HKCU. *keyname* es el nombre de clave. *value* es un mandato opcional que especifica el valor del registro que se migra.	Especifica el directorio de instalación tal como aparece en el registro.
<Files_From_Folders> Opcional			

Tabla 12. (continuación)

Sección	Mandato	Valor	Qué hace

	SMAVariable\Location[|File][/s]
	
	donde
	• SMAvariable es una de las variables siguientes que especifican la ubicación de los archivos de personalización:
	– %Windows Directory% (ubicación de los archivos del sistema operativo)
	– %Install Directory% (ubicación de la aplicación tal como está definida en a sección Install_Directories)
	– %Appdata Directory% (directorio de los datos de la aplicación, que es un subdirectorio del directorio de perfil de usuario)
	– %LocalAppdata Directory% (directorio de los datos de la aplicación en la carpeta Local Settings, que es un subdirectorio del directorio del perfil de usuario)
	– %Cookies Directory% (directorio Cookies, que es un subdirectorio del directorio del perfil de usuario)
	– %Favorites Directory% (directorio Favorites, que es un subdirectorio del directorio del perfil de usuario)
	– %%Personal Directory% (directorio Personal, que es un subdirectorio (My Documents) del directorio del perfil de usuario. Esta variable de entorno no puede ser utilizada por Windows NT4.)
			Especifica los archivos de personalización que desea migrar.
			
			Por ejemplo:
			`<Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi</Files_And_Folders>`
			
			SMA captura los archivos en la carpeta %AppData Directory%\Adobe\Acrobat\Whapi.
			
			Los archivos de los subdirectorios no se incluyen.
			`<Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi\ /s</Files_From_Folder>`
			
			SMA captura los archivos en la carpeta %AppData Directory%\Adobe\Acrobat\Whapi. Los archivos de los subdirectorios se incluyen.
			`<Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi\*.*</Files_From_Folder>`
			
			SMA captura los archivos en la carpeta %AppData Directory%\Adobe\Acrobat\Whapi. Los archivos de los subdirectorios no se incluyen.
			`<Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi\*.* /s</Files_From_Folder>`
			
			SMA captura los archivos en la carpeta %AppData Directory%\Adobe\Acrobat\Whapi. Los archivos de los subdirectorios se incluyen.
			`<Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi</Files_From_Folder>`
			
			Cuando "\" no va a continuación de "Whapi", SMA trata "Whapi" no como una carpeta sino como un archivo.

Tabla 12. (continuación)

Sección	Mandato	Valor	Qué hace
	• *Location* especifica un archivo o un directorio totalmente calificado. Puede utilizar caracteres comodín en el nombre de archivo pero no en la vía de acceso. Si especifica un directorio, todos los archivos se copiarán. • *[File]* es un parámetro opcional que sólo se puede utilizar si Location especifica un directorio y File es el archivo que se debe copiar. Puede utilizar caracteres comodín en el nombre de archivo pero no en la vía de acceso. • *[/s]* es un parámetro opcional. Si utiliza [/s], se copiarán todos los archivos de los subdirectorios. • El usuario de SMA5.0 puede utilizar la variable de entorno de Windows. La variable de entorno del usuario que ha iniciado SMA se utiliza como el valor de la variable de entorno de Windows.		
<Registries> Opcional			

	hive es HKLM o HKCU.
	
	keyname es el nombre de clave.*value* es un mandato opcional que especifica el valor del registro que se migra.
			Especifica las entradas del registro que desea migrar.
			
			Por ejemplo:
			`<Registries>`
			`<Registry>`
			`<hive>HKCU</hive>`
			`<keyname>Software\Adobe\Acrobat</keyname>`
			`<value></value>`
			`</Registry>`
			`</Registries>`

<Registry_Excludes> Opcional			

	hive es HKLM o HKCU.
	
	keyname es el nombre de clave.*value* es un mandato opcional que especifica el valor del registro que se migra.
			Especifica las claves y los valores de registro que desea excluir de las entradas de registro seleccionadas.
			
			Por ejemplo:
			`<Registry_Excludes>`
			`<Registry>`
			`<hive>HKCU</hive>`
			`<keyname>Software\Adobe\Acrobat Reader\5.0\AdobeViewer`
			`</keyname>`
			`<value>xRes</value>`
			`</Registry>`
			`</Registry_Excludes>`

<Files_Through_Registry>			

Tabla 12. (continuación)

Sección	Mandato	Valor	Qué hace
	<OS> Especifica el sistema operativo y tiene uno de los valores siguientes: • WinXP • Win2000 • WinNT • Win98 <Registry> especifica la entrada de registro y tiene el formato hive,nombreclave,valor, donde: • hive es HKLM o HKCU. • nombreclave es el nombre de la clave. • valor es un mandato opcional que especifica el valor del registro que se migra. File es el nombre del archivo. Puede utilizar caracteres comodines. File es el nombre del archivo. Puede utilizar caracteres comodines.		Especifica los archivos de personalización que se migrarán Por ejemplo: <Files_Through_Registries> <Files_Through_Registry> <OS>WinXP</OS> <Registry> <hive>HKCU</hive> <keyname>Software\Lotus\Organizer\99.0\Paths</keyname> <value>Backup</value> </Registry> <File>*.*/s</File> </Files_Through_Registry> </Files_Through_Registries>
<PreTargetBatchProcessing>			
	<PreTargetBatchProcessing> <!CDAT[batch commands]] <PreTargetBatchProcessing>		<PreTargetBatchProcessing> realiza proceso por lotes antes de que Apply procese <Registries>. Por ejemplo: <PreTargetBatchProcessing> <!CDATA[copy /y c:\temp*.* c:\migration del c:\migration*.mp3 </PreTargetBatchProcessing>
<TargetBatchProcessing>			
	<TargetBatchProcessing> <!CDAT[batch commands]] <TargetBatchProcessing>		<TargetBatchProcessing> realiza proceso por lotes antes de que Apply procese <Registries>. Por ejemplo: <TargetBatchProcessing> <!CDATA[copy /y c:\temp*.* c:\migration del c:\migration*.mp3 <TargetBatchProcessing>

Creación de un archivo de aplicación

Para determinar los valores de la aplicación que se deben migrar para los archivos de aplicación personalizados, debe probar cuidadosamente las aplicaciones.

Complete los pasos siguiente para crear un archivo de migración:

1. Utilice un editor de texto ASCII para abrir un archivo aplicación.XML existente. Si ha instalado SMA en la ubicación por omisión, los archivos aplicación.XML están ubicados en el directorio d:\%RR%\Migration\bin\Apps, donde d es la letra de la unidad de la unidad de disco duro.

2. Modifique el archivo aplicación.XML para la aplicación y los valores de las aplicaciones que desee migrar.
3. Modifique la información en la sección <Applications>.
4. Modifique los mandatos <Name> y <Version> de la sección <Application Shortname=*NombreCorto*.
5. Determine las claves de registro que se deben migrar:
   a. Pulse **Inicio → Ejecutar**. Se abrirá la ventana "Run". En el campo **Abrir**, escriba regedit y pulse **Aceptar**. Se abrirá la ventana "Editor de registro".
   b. En el primer panel, expanda el nodo **HKEY_LOCAL_MACHINE**.
   c. Expanda el nodo **Software**.
   d. Expanda el nodo específica del proveedor, por ejemplo, **Adobe**.
   e. Continúe navegando hasta que haya localizado la clave de registro para la aplicación. En este ejemplo, la clave de registro es SOFTWARE\Adobe\Acrobat Reader\6.0.
   f. Establezca el valor del campo Detect. Por ejemplo:

```
<Detects>
<Detect
<hive>HKLM</hive>
<keyname>Software\Adobe|acrobat Reader\6.0<keyname>
</Detect
</Detects
```

6. Modifique los mandatos Name y Version de la sección Install_Directories.
7. Determine la vía de acceso de los directorios de instalación para la aplicación.
   a. En la ventana "Registry Editor", navegue hasta el nodo HKLM\SOFTWARE\Adobe\Acrobat Reader\6.0\InstallPath.
   b. Añada el mandato adecuado a la sección Install_Directories del archivo de aplicación. Por ejemplo:

```
<Install_Directory>
<OS>WinXP</OS>
<Registry>
<hive>HKLM</hive
<keyname>Software\Adobe\Acrobat Reader\6.0\InstallPath</keyname>
<value>(Default)</value>
</Registry>
</Install_Directory>
```

   Nota: Si no encuentra un directorio específico de la aplicación en el directorio HKLM\Software\Microsoft\Windows\CurrentVersion\AppPaths, debe localizar un directorio que contenga la vía de acceso de instalación en algún otro lugar del árbol HKLM\Software. A continuación, utilice esa clave en la sección <Install_Directories>
8. En la sección <Files_From Folders>, especifique los archivos de personalización que desee migrar.
   a. Debido a que muchas aplicaciones por omisión guardan archivos en el subdirectorio Documents and settings, compruebe si en el directorio de datos de las aplicaciones hay directorios que pertenezcan a la aplicación. Si existe uno, puede utilizar el mandato siguiente para migrar el directorio y los archivos:

```
<Files_From_Folder>SMAvariable\Location\[File] [/s] </Files_From_Folder>
```

   donde Location/ es un archivo o directorio totalmente calificado y [File] es un parámetro opcional que se puede utilizar sólo si Location/ especifica

un directorio. En el ejemplo de Adobe Reader, los archivos de personalización están en el directorio Preferences.

b. Compruebe todos los directorios relacionados ya que es posible que los valores personales estén almacenados allí.

c. Compruebe el directorio Local Settings.

9. Determine las entradas de registro que desea migrar. Estarán en HKCU (HKEY_CURRENT_USER). En la sección <Registries> del archivo de aplicación, añada los mandatos adecuados.
10. Guarde el archivo aplicación.XML en el directorio d:\Archivos de programa\ThinkVantage\SMA\Apps, donde d es la letra de la unidad de disco duro.
11. Pruebe el nuevo archivo de aplicación.

Ejemplo de un archivo aplicación.XML para Adobe Reader

Esta sección contiene un archivo de aplicación para Adobe Reader.

```
<?xml version="1.0"?>
<Applications>
<Family>Adobe Acrobat Reader</Family>
<SMA_Version>SMA 5.0</SMA_Version>
<APP>Acrobat_Reader_70</APP>
<APP>Acrobat_Reader_60</APP>
<APP>Acrobat_Reader_50</APP>

<Application ShortName="Acrobat_Reader_50">
<AppInfor>
         <Name>Acrobat_Reader_50</Name>
         <Version>5.0</Version>
         <Detects>
                 <Detect>
                     <hive>HKLM</hive>
                     <keyname>Software\Adobe\Acrobat Reader\5.0</keyanme>
                 </Detect>
         </Detects>
</AppInfo>
<Install_Directories>
            <Install_Directory>
               <OS>WinXP</OS>
               <Registry>
                        <hive>HKLM</hive>
                        <keyname>Software\Adobe\Acrobat Reader\5.0\InstallPath
</keyname>
                        <value>(Default)</value>
               </Registry>
            </Install_Directory>
            <Install_Directory>
               <OS>Win2000</OS>
               <Registry>
                        <hive>HKLM</hive>
                        <keyname>Software\Adobe\Acrobat Reader\5.0\InstallPath
</keyname>
                        <value>(Default)</value>
               </Registry>
            </Install_Directory>
            <Install_Directory>
                 <OS>Win98</OS>
                 <Registry>
                        <hive>HKLM</hive>
                        <keyname>Software\Adobe\Acrobat Reader\5.0\InstallPath
<keyname>
                        <value>(Default)</value>
                 </Registry>
            </Install_Directory>
```

```
            <Install_Directory>
                 <OS>WinNT</OS>
                 <Registry>
                       <hive>HKLM</hive>
                       <keyname>Software\Adobe\Acrobat Reader\5.0\InstallPath
</keyname>
                       <value>(Default)</value>
                 </Registry>
            </Install_Directory>
</Install_Directories>

<Files_From_Folders>
           <Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi\*.*
/s</Files_From_Folder>
           <Files_From_Folder>%Personal Directory%\*.pdf</Files_From_Folder>
<Files_From_Folders>
<Files_Through_Registries>
</Files_Through_Registries>

<Registries>
            <Registry>
                       <hive>HKCU</hive>
                       <keyname>Software\Adobe\Acrobat</keyname>
             </Registry>
             <Registry>
                       <hive>HKCU</hive>
                       <keyname>Software\Adobe\Acrobat Reader</keyname>
             </Registry>
             <Registry>
                       <hive>HKCU</hive>
                       <keyname>Software\Adobe\Persistent Data</keyname>
             </Registry>
</Registries>

<Registry_Excludes>
            <Registry>
                       <hive>HKCU</hive>
                       <keyname>Software\Adobe\Acrobat Reader\5.0\AdobeViewer
</keyname>
                       <value>xRes</value>
            </Registry>
            <Registry>
                       <hive>HKCU</hive>
                       <keyname>Software\Adobe\Acrobat Reader\5.0\Adobe\Viewer
</keyname>
                       <value>yRes</value>
            </Registry>
<Registry_Excludes>

<SourceBatchProcessing>
</SourceBatchProcessing>

<PreTargetBatchProcessing>
</PreTargetBatchProcessing>

<TargetBatchProcessing> </TargetBatchProcessing>
</Application>
<Application ShortName="Acrobat_Reader_6.0">
        <AppInfo>
                    <Name>Adobe Acrobat Reader 6.0<\Name>
                           <Version>6.0</Version>
                           <Detects>
                                 <Detect>
                                        <hive>HKLM</hive>
                                        <keyname>Software\Adobe\Acrobat Reader\6.0
</keyname>
                                 </Detect>
```

```
                        </Detects>
        <\AppInfo>
<Install_Directories>
          <Install_Directory>
               <OS>WinXP</OS>
               <Registry>
                         <hive>HKLM</hive>
                         <keyname>Software\Adobe\Acrobat Reader\6.0\InstallPath
</keyname>
                         <value>(Default)</value>
               </Registry>
          </Install_Directory>
          <Install_Directory>
               <OS>Win2000</OS>
               <Registry>
                         <hive>HKLM</hive>
                         <keyname>Software\Adobe\Acrobat Reader\6.0\InstallPath
</keyname>
                         <value>(Default)</value>
               </Registry>
          </Install_Directory>
          <Install_Directory>
              <OS>Win98</OS>
              <Registry>
                         <hive>HKLM</hive>
                         <keyname>Software\Adobe\Acrobat Reader\6.0\InstallPath
</keyname>
                         <value>(Default)</value>
             </Registry>
         </Install_Directory><Install_Directory>
             <OS>WinNT</OS>
             <Registry>
                       <hive>HKLM</hive>
                       <keyname>Software\Adobe\Acrobat Reader\6.0\InstallPath
</keyname>
                       <value>(Default)</value>
             </Registry>
         </Install_Directory>
</Install_Directories>

<Files_From_Folders>
            <Files_From_Folder>%AppData Directory%\Adobe\Acrobat\6.0\*.* /s
</Files_From_Folder>
            <Files_From_Folder>%Personal Directory%\*.pdf</Files_From_Folder>
</Files_From_Folders>

<Files_Trough_Registries>
</Files_Trough_Registries>

<Registries>
             <Registry>
                       <hive>HKCU</hive>
                       <keyname>Software\Adobe\Acrobat</keyname>
             </Registry>
             <Registry>
                       <hive>HKCU</hive>
                       <keyname>Software\Adobe\Acrobat Reader</keyname>
             </Registry>
</Registries>

<Registry_Excludes>
             <Registry>
                       <hive>HKCU</hive>
                       <keyname>Software\Adobe\Acrobat Reader\6.0\AdobeViewer
</keyname>
                       <value>xRes</value>
             </Registry>
```

```
            <Registry>
                      <hive>HKCU</hive>
                      <keyname>Software\Adobe\Acrobat Reader\6.0\Adobe\Viewer
</keyname>
                      <value>yRes</value>
            </Registry>
<Registry_Excludes>

<SourceBatchProcessing>
</SourceBatchProcessing>

<PreTargetBatchProcessing>
</PreTargetBatchhProcessing>

<TargetBatchProcessing>            <![CDATA[
          if /i "%SourceApp%" == "Acrobat_Reader_50" goto Update50
          goto Done
          :Update50
          regfix "HKCU\Software\Adobe\Acrobat Reader\5.0" "HKCU\Software\Adobe\
Acrobat Reader\6.0"
          regfix "HKLM\Software\Adobe\Acrobat Reader\5.0\AdobeViewer" "HKLM\
Software\Adobe\Acrobat Reader\6.0\AdobeViewer"
          :Done
]]>
</TargetBatchProcessing>
</Application>

<Application ShortName="Acrobat_Reader_7.0">
             <AppInfo>
                       <Name>Adobe Acrobat Reader 7.0<\Name>
                       <Version>6.0</Version>
                       <Detects>
                                <Detect>
                                <hive>HKLM</hive>
                                <keyname>Software\Adobe\Acrobat Reader
\7.0</keyname>
                                </Detect>
                       </Detects>
            <\AppInfo>
<Install_Directories>
             <Install_Directory>
                          <OS>WinXP</OS>
                          <Registry>
                                <hive>HKLM</hive>
                                <keyname>Software\Adobe\Acrobat Reader\7.0\
InstallPath</keyname>
                                <value>(Default)</value>
                          </Registry>
             </Install_Directory>
             <Install_Directory>
                          <OS>Win2000</OS>
                          <Registry>
                                    <hive>HKLM</hive>
                                    <keyname>Software\Adobe\Acrobat Reader\7.0\
InstallPath</keyname>
                                    <value>(Default)</value>
                          </Registry>
             </Install_Directory>
<Install_Directory>
                          <OS>Win98</OS>
                          <Registry>
                                    <hive>HKLM</hive>
                                    <keyname>Software\Adobe\Acrobat Reader\7.0\
InstallPath</keyname>
                                    <value>(Default)</value>
                          </Registry>
             </Install_Directory><Install_Directory>
```

```
                        <OS>WinNT</OS>
                        <Registry>
                                 <hive>HKLM</hive>
                                 <keyname>Software\Adobe\Acrobat Reader\7.0\
InstallPath</keyname>
                                 <value>(Default)</value>
                         </Registry>
             </Install_Directory>
</Install_Directories>

<Files_From_Folders>
           <Files_From_Folder>%AppData Directory%\Adobe\Acrobat\7.0\*.* /s
</Files_From_Folder>
           <Files_From_Folder>%Personal Directory%\*.pdf</Files_From_Folder>
</Files_From_Folders>

<Files_Trough_Registries>
</Files_Trough_Registries>

<Registries>
           <Registry>
                     <hive>HKCU</hive>
                     <keyname>Software\Adobe\Acrobat</keyname>
           </Registry>
           <Registry>
                     <hive>HKCU</hive>
                     <keyname>Software\Adobe\Acrobat Reader</keyname>
           </Registry>
</Registries>

<Registry_Excludes>
           <Registry>
                     <hive>HKCU</hive>
                     <keyname>Software\Adobe\Acrobat Reader\7.0\AdobeViewer
</keyname>
                     <value>xRes</value>
           </Registry>
           <Registry>
                     <hive>HKCU</hive>
                     <keyname>Software\Adobe\Acrobat Reader\7.0\Adobe\Viewer
</keyname>
                     <value>yRes</value>
           </Registry>
<Registry_Excludes>

<SourceBatchProcessing>
</SourceBatchProcessing>

<PreTargetBatchProcessing>
</PreTargetBatchProcessing>

TargetBatchProcessing>
           <![CDATA[
          if /i "%SourceApp%" == "Acrobat_Reader_50" goto Update50
          if /i "%SourceApp%" == "Acrobat_Reader_60" goto Update60
          goto Done
          :Update50
          regfix "HKCU\Software\Adobe\Acrobat Reader\5.0" "HKCU\Sof
tware\Adobe\Acrobat Reader\7.0"
          regfix "HKLM\Software\Adobe\Acrobat Reader\5.0\AdobeView
er" "HKLM\Software\Adobe\Acrobat Reader\7.0\AdobeViewer"
          goto Done
          :Update60
regfix "HKCU\Software\Adobe\Acrobat Reader\6.0" "HKCU\Softw
are\Adobe\Acrobat Reader\7.0"
          regfix "HKLM\Software\Adobe\Acrobat Reader\6.0\AdobeVi
ewer" "HKLM\Software\Adobe\Acrobat Reader\7.0\AdobeViewer"
```

```
          :Done
          ]]>
</TargetBatchProcessing>
</Application>

</Applications>
```

Actualización del sistema

Active Update

Para determinar si Active Update Launcher está instalado, compruebe si existe la siguiente clave de registro:

```
HKLM\Software\TVT\ActiveUpdate
```

Para determinar si Active Update Launcher está configurado correctamente para permitir la actualización activa, TVT comprueba en su propia clave de registro el valor del atributo EnableActiveUpdate. Si EnableActiveUpdate=1, TVT añade el elemento de menú ActiveUpdate debajo del menú Ayuda.

Para llamar a Active Update, el TVT que realiza la llamada inicia el programa Active Update Launcher y pasa un archivo de parámetros.

Utilice los pasos siguientes para invocar a Active Update:

1. Abra la clave de registro de Active Update Launcher:
   ```
   HKLM\software\TVT\ActiveUpdate
   ```
2. Obtenga el valor del atributo Path.
3. Obtenga el valor del atributo Program.

Capítulo 6. Instalación

El paquete de instalación de Rescue and Recovery/Client Security Solution se ha desarrollado con InstallShield 10.5 Premier como un proyecto MSI básico. Los proyectos MSI Básico de InstallShield 10.5 utilizan Windows Installer para instalar aplicaciones, lo que proporciona a los administradores muchas posibilidades para personalizar instalaciones, como por ejemplo establecer valores de propiedades desde la línea de mandatos. Las secciones siguientes describen formas de utilizar y ejecutar el paquete de instalación de Rescue and Recovery 3.0. Para una mejor mejor comprensión, lea primero todo el capítulo antes de empezar a instalar el paquete.

Nota: Al instalar este paquete, consulte por favor el archivo Readme que se puede encontrar en la página Web de Lenovo en:

www.Lenovo.com/ThinkVantage

El archivo Readme contiene información actualizada acerca de temas como las versiones de software, los sistemas soportados, los requisitos del sistema y otras consideraciones para ayudarle con el proceso de instalación.

Requisitos de instalación

Esta sección trata sobre los requisitos del sistema para instalar el paquete de Rescue and Recovery/Client Security Solution. Para obtener mejores resultados, vaya al siguiente sitio Web para asegurarse de que tiene la versión más reciente del software:

www.Lenovo.com/ThinkVantage

Una serie de sistemas antiguos de IBM pueden dar soporte de Rescue and Recovery, siempre que cumplan los requisitos especificados. Consulte la página de descarga en la Web para obtener información acerca de sistemas no IBM que permiten Rescue and Recovery.

Requisitos para sistemas IBM y Lenovo

Los sistemas IBM y Lenovo deben satisfacer como mínimo los siguientes requisitos para poder ejecutar Rescue and Recovery:

- Sistema operativo: Microsoft Windows XP o Windows 2000
- Procesador: El que especifica Microsoft para Windows XP (Home o Professional) y Windows 2000
  - Service Pack 1, como mínimo
- Memoria: 128 MB
  - En configuraciones de memoria compartida, el valor del BIOS para el máximo de memoria compartida se debe establecer en un valor que no sea inferior a 4 MB ni superior a 8 MB.
  - En configuraciones de memoria no compartida, 120 MB de memoria no compartida.

    Nota: Si un sistema tiene menos de 200 MB de memoria no compartida, Rescue and Recovery se ejecutará. Sin embargo, es posible que el usuario no pueda iniciar mas de una aplicación en el entorno de Rescue and Recovery.

- 1,5 GB de espacio libre de disco duro (la instalación base requiere 930 MB y no incluye espacio necesario para las copias de seguridad de Rescue and Recovery)
- Vídeo compatible con VGA que dé soporte a la resolución de 800 x 600 y de 24 bits color
- Tarjeta Ethernet soportada

Requisitos para instalar y utilizar sistemas que no sean Lenovo ni IBM

La instalación en sistemas que no sean IBM ni Lenovo tiene los requisitos siguientes:

Requisitos de instalación

1,5 GB de espacio libre de disco. La instalación base utiliza 930 MB.

Requisitos mínimos de memoria del sistema

El sistema que no es IBM ni Lenovo debe tener una RAM del sistema de 128 MB para instalar Rescue and Recovery.

Configuración de la unidad de disco duro

El programa Rescue and Recovery no está soportado en las precargas de fábrica para sistemas del fabricante del equipo original (OEM) (no IBM ni Lenovo). Para sistemas OEM, la unidad de disco duro debe estar configurada según las recomendaciones de "Instalación de Rescue and Recovery en sistemas no IBM" en la página 133.

Adaptadores de red

El entorno de Rescue and Recovery da soporte solamente a adaptadores de red Ethernet, basados en PCI, por cable. Los controladores de red incluidos en el entorno de Rescue and Recovery son los mismos controladores que se incluyen en el sistema operativo Microsoft Windows XP Professional y son independientes del sistema operativo Windows. Para sistemas Lenovo e IBM soportados, los controladores necesarios se incluyen con el software de Rescue and Recovery.

Si un dispositivo de red OEM del sistema no está soportado, consulte la documentación que se proporcionaba con el dispositivo para obtener instrucciones acerca de cómo añadir soporte para controladores de red específicos del sistema. Solicite controladores del OEM.

Soporte del arranque desde un soporte externo (CD/DVD y USB)

Los sistemas y los dispositivos (unidad de disco duro USB, CD-R/RW, DVD-R/RW/RAM o DVD+R/RW) que no son IBM ni Lenovo deben dar soporte a una de las especificaciones siguientes:

- Especificación de BIOS de dispositivo de soporte extraíble ATAPI
- Servicios de unidad de disco mejorado de BIOS - 2
- Especificación de arranque de BIOS de Compaq Phoenix Intel
- Especificaciones del formato de CD-ROM de arranque de El Torito
- Visión general de la especificación de clase de almacenamiento masivo USB (cada dispositivo debe cumplir la especificación de bloque de mandatos en la sección 2.0 del código de subclase de ″USB Mass Storage Class Specification Overview.″)
- Especificación de almacenamiento masivo USB para la capacidad de arranque

Requisitos de vídeo

- **Compatibilidad de vídeo:** Vídeo compatible con VGA que permite una resolución de 800 x 600 y color de 24 bits
- **Memoria de vídeo:**

– En sistemas de memoria de vídeo no compartida: un mínimo de 4 MB de RAM de vídeo
– En sistemas de memoria de vídeo compartida: un mínimo de 4 MB y un máximo de 8 MB se pueden asignar para la memoria de vídeo.

Compatibilidad de la aplicación

Es posible que algunas aplicaciones que tienen entornos de controladores de filtro complejos (como por ejemplo el software antivirus) no sean compatibles con el software de Rescue and Recovery. Para obtener información acerca de los temas de compatibilidad, consulte el archivo README que acompaña al software de Rescue and Recovery en la Web:

www.lenovo.com/ThinkVantage

Programas de utilidad

Esta guía hace referencia a una serie de programas de utilidad. Estos programas de utilidad se pueden encontrar en este sitio Web:

www.Lenovo.com/ThinkVantage

Componentes de la instalación de Rescue and Recovery

1. Paquete de instalación principal (aproximadamente 45 MB): es el archivo setup.exe creado a partir de la fuente del proyecto de instalación. El nombre del archivo setup.exe se cambia durante el proceso de creación a un nombre que representa el ID del proyecto, el tipo de soporte, el nivel de build, el código de país (siempre US en este caso) y el código de parche – por ejemplo, Z096ZIS1001US00.exe. Se trata de un paquete de instalación autoextraíble que extrae los archivos fuente de la instalación e inicia la instalación utilizando Windows Installer. Contiene la lógica de la instalación y los archivos de las aplicaciones de Windows. El paquete no contiene ninguno de los archivos del área previa al escritorio.
2. Base US del Área previa al escritorio (aproximadamente 135 MB): es el archivo zip protegido mediante contraseña que contiene toda la base US del área previa al escritorio. Su nombre tiene el formato Z062ZAA1001US00.TVT, donde *AA* determina la compatibilidad del área previa al escritorio y *001* es el nivel del área previa al escritorio. Este archivo es necesario para instalar el área previa al escritorio en sistemas de cualquier idioma. Este archivo debe estar en el mismo directorio que el paquete de instalación principal (setup.exe o Rescue and Recovery/Client Security Solution.msi si se ha extraído o la instalación OEM). Excepciones a esto son si el área previa al escritorio ya está instalada y no es necesario actualizarla o bien si la propiedad PDA=0 está establecida en la línea de mandatos al ejecutar la instalación y el área previa al escritorio (cualquier versión) no existe aún. El archivo setup.exe contiene un archivo pdaversion.txt que contiene la versión mínima del área previa al escritorio que puede funcionar con esa versión de Windows. El instalador de setup.exe buscará el archivo del área previa al escritorio utilizando la lógica siguiente:
   - **Existe una versión antigua del área previa al escritorio (RNR 1.0 ó 2.X) o no existe ninguna:**

     El instalador buscará un archivo .TVT con un código de compatibilidad (por ejemplo, AA, AB) que equivalga al código de compatibilidad de versión mínima y un nivel que sea mayor que o igual a la versión mínima (todos los demás campos de versión en el nombre de archivo .TVT deben coincidir exactamente con la versión mínima). Si no se encuentra un archivo que satisfaga estos criterios, la instalación se detendrá.

- **Existe una nueva área previa al escritorio (RNR 3.0):**

  El instalador comparará el código de compatibilidad del área previa al escritorio actual con el código de compatibilidad de la versión mínima y realizará las acciones siguientes en base a los resultados:

  – Código **actual > Código mínimo:**

    El instalador presentará un mensaje indicando que el entorno actual no es compatible con esta versión de RNR.

  – Código **actual = Código mínimo:**

    El instalador compara el nivel de versión actual con el nivel de versión mínima. Si el nivel actual es mayor que o igual al nivel mínimo, el instalador busca un archivo .TVT con un código de compatibilidad (AA, AB...) que sea equivalente al código de compatibilidad de versión mínima y un nivel que sea mayor que el nivel de versión actual (todos los demás campos de versión del nombre de archivo .TVT deben coincidir exactamente con la versión mínima). Si no encuentra ningún archivo, el proceso de instalación continúa sin actualizar el área previa al escritorio. Si el nivel actual es inferior al nivel mínimo, el instalador buscará un archivo .TVT con un código de compatibilidad (AA, AB,...) que equivalga al código de compatibilidad de versión mínima y un nivel que sea mayor que o igual al nivel de versión mínima (todas las demás campos de versión del nombre de archivo .TVT deben coincidir exactamente con la versión mínima). Si no se encuentra un archivo que satisfaga estos criterios, la instalación se detendrá.

  – Código **actual > Código mínimo:**

    El instalador buscará un archivo .TVT con un código de compatibilidad (AA, AB,...) que equivalga al código de compatibilidad de versión mínima y a un nivel que sea mayor que o igual a la versión mínima (todos los demás campos de versión del nombre de archivo .TVT deben coincidir exactamente con la versión mínima). Si no se encuentra un archivo que satisfaga estos criterios, la instalación se detendrá.

3. Los paquetes de idioma del Área previa al escritorio (aproximadamente 5 – 30 MB cada uno): Son 24 paquetes de idioma para Windows PE que están soportados en Rescue and Recovery 3.0. Cada paquete de idioma recibe un nombre con el formato Z062ZAA1001CP00.TVT donde CP representa el idioma. Es necesario uno de estos archivos si el Área previa al escritorio está siendo instalada en un sistema distinto del inglés o en un sistema con un idioma no soportado y y debe estar en el mismo directorio que la instalación principal y que el archivo .TVT US del Área previa al escritorio. El idioma del paquete de idioma debe coincidir con el idioma de Windows, si Windows no está en inglés o está en un idioma no soportado por los paquetes de idioma. Si el Área previa al escritorio se está instalando o actualizando y es necesario un paquete de idioma, la instalación busca un paquete de idioma .TVT donde todos los campos del nombre de archivo coincidan con el nombre de archivo del Área previa al escritorio US excepto el código de país que debe coincidir con el idioma del sistema. Los paquetes de idioma están disponibles en los idiomas siguientes:
   - Árabe
   - Portugués de Brasil
   - Portugués
   - Checo
   - Danés
   - Finlandés

- Francés
- Griego
- Alemán
- Hebreo
- Chino de Hong Kong
- Húngaro
- Italiano
- Japonés
- Coreano
- Holandés
- Noruego
- Polaco
- Portugués
- Ruso
- Chino simplificado
- Español
- Sueco
- Chino tradicional
- Turco

Procedimiento de instalación estándar y parámetros de la línea de mandatos

Setup.exe puede aceptar un conjunto de parámetros de la línea de mandatos, los cuales se describen a continuación. Las opciones de la línea de mandatos que requieren un parámetro se deben especificar sin ningún espacio entre la opción y su parámetro. Por ejemplo, Setup.exe /s /v"/qn REBOOT="R"" es válido, mientras que Setup.exe /s /v "/qn REBOOT="R"" no lo es. Es necesario que el parámetro de la opción esté entre comillas dobles sólo si el parámetro contiene espacios.

Nota: Por omisión, la instalación cuando se ejecuta sola (simplemente ejecutando setup.exe sin ningún parámetro) solicita al usuario que rearranque al final de la instalación. Es necesario rearrancar para que el programa funcione correctamente. Se puede aplazar el rearranque mediante un parámetro de la línea de mandatos para una instalación silenciosa, tal como se ha explicado anteriormente y en la sección de ejemplo.

Los parámetros y las descripciones siguientes se han tomado directamente de la documentación de ayuda del desarrollador de InstallShield. Se han eliminado los parámetros que no son aplicables a proyectos de MSI básico.

Tabla 13.

Parámetro	Descripción
/a : Instalación administrativa	El conmutador /a hace que setup.exe realice una instalación administrativa. Una instalación administrativa copia (y descomprime) los archivos de datos en un directorio especificado por el usuario, pero no crea atajos, registra servidores COM ni crea un registro de desinstalación.

Tabla 13. (continuación)

Parámetro	Descripción
/x : Modalidad de desinstalación	El conmutador /x hace que setup.exe desinstale un producto instalado anteriormente.
/s : Modalidad silenciosa	El mandato setup.exe /s suprime la ventana de inicialización de setup.exe para un programa de instalación MSI básico, pero no lee un archivo de respuestas. Los proyectos MSI básico no crean ni utilizan un archivo de respuestas para las instalaciones silenciosas. Para ejecutar un producto de MSI básico de forma silenciosa, ejecute la línea de mandatos setup.exe /s /v/qn. (Para especificar los valores de las propiedades públicas para una instalación MSI básico silenciosa, puede utilizar un mandato como por ejemplo setup.exe /s /v"/qn INSTALLDIR=D:\Destino".)
/v : pasa argumentos a Msiexec	El argumento /v se utiliza para pasar conmutadores de la línea de mandatos y valores de propiedades públicas a Msiexec.exe.
/L : configura el idioma	Los usuarios pueden utilizar el conmutador /L con el ID decimal de idioma para especificar el idioma utilizado por el programa de instalación en varios idiomas. Por ejemplo, el mandato para especificar alemán es setup.exe /L1031. Nota: No todos los idiomas a los que se hace referencia en la Tabla 14 están soportados en la instalación.
/w : Espera	Para un proyecto MSI básico, el argumento /w obliga a setup.exe a esperar hasta que se complete la instalación antes de salir. Si está utilizando la opción /w en un archivo de proceso por lotes, es posible que desee anteponer start /WAIT a todo el argumento de la línea del mandato setup.exe. A continuación se muestra un ejemplo correctamente formado de este uso: `start /WAIT setup.exe /w`

Tabla 14.

Idioma	Identificador
Árabe (Arabia Saudí)	1025
Vasco	1069
Búlgaro	1026
Catalán	1027
Chino simplificado	2052
Chino tradicional	1028
Croata	1050
Checo	1029

Tabla 14. (continuación)

Idioma	Identificador
Danés	1030
Holandés (estándar)	1043
Inglés	1033
Finlandés	1035
Francés de Canadá	3084
Francés	1036
Alemán	1031
Griego	1032
Hebreo	1037
Húngaro	1038
Indonesio	1057
Italiano	1040
Japonés	1041
Coreano	1042
Noruego (Bokmal)	1044
Polaco	1045
Portugués (Brasil)	1046
Portugués (estándar)	2070
Rumano	1048
Ruso	1049
Eslovaco	1051
Esloveno	1060
Español	1034
Sueco	1053
Tailandés	1054
Turco	1055

Procedimiento de instalación administrativo y parámetros de la línea de mandatos

Windows Installer puede realizar una instalación administrativa de una aplicación o de un producto en una red para que éste sea utilizado por un grupo de trabajo o para la personalización del mismo. Para el paquete de instalación de Rescue and Recovery/Client Security Solution, una instalación administrativa desempaqueta los archivos fuente de instalación en una ubicación específica. Para ejecutar una instalación administrativa, es necesario ejecutar el paquete de instalación desde la línea de mandatos utilizando el parámetro /a:

```
Setup.exe /a
```

El inicio de la instalación administrativa presenta una serie de pantallas de diálogo que solicitan al usuario administrativo que especifique una ubicación donde desempaquetar los archivos de instalación. La ubicación de extracción por omisión que se presenta al usuario administrativo es C:\. Se puede seleccionar una nueva

ubicación que puede incluir unidades que no sean la unidad C: (por ejemplo, otras unidades locales o unidades de red correlacionadas). También se pueden crear nuevos directorios durante este paso.

Si se ejecuta de forma silenciosa una instalación administrativa, se puede establecer en la línea de mandatos la propiedad pública TARGETDIR para que especifique la ubicación de extracción:

```
Setup.exe /s /v"/qn TARGETDIR=F:\TVTRR"
```

Una vez que se haya completado una instalación administrativa, el usuario administrativo puede realizar personalizaciones en los archivos fuente; por ejemplo, añadir valores adicionales a tvt.txt. Para instalar a partir de las fuentes desempaquetadas después de que se hayan realizado personalizaciones, el usuario llama a msiexec.exe desde la línea de mandatos, pasando el nombre del archivo msi desempaquetado.

La sección siguiente describe los parámetros de la línea de mandatos disponibles que se pueden utilizar con msiexec, así como un ejemplo de cómo utilizarlos. Las propiedades públicas también se pueden establecer directamente en la llamada de la línea de mandatos de msiexec.

Parámetros de la línea de mandatos de msiExec.exe

MsiExec.exe es un programa ejecutable de Windows Installer utilizado para interpretar los paquetes de instalación e instalar productos en los sistemas de destino:

```
msiexec. /i "C:CarpetaWindows/Perfiles\NombreUsuario\Personal\MisValores\nombre
proyecto\configuración del producto\nombre de release\DiskImages\Disk1\nombre
del producto.msi
```

La tabla siguiente proporciona una descripción detallada de los parámetros de la línea de mandatos de msiExec.exe. Esta tabla se toma directamente de la documentación de Microsoft Platform SDK de Windows Installer.

Tabla 15.

Parámetro	Descripción
/i *paquete* o *código del producto*	Utilice este formato para instalar el producto Othello: `msiexec /i "C:\CarpetaWindows\Perfiles\ NombreUsuario\Personal\MisValores\Othello\ Versión de prueba\Release\ImágenesDisco\Disco1\ Othello Beta.msi"` El código del producto se refiere a la GUI que se genera automáticamente en la propiedad del Código del producto de la vista de proyectos del producto.

Tabla 15. (continuación)

Parámetro	Descripción
/f [p|o|e|d|c|a|u|m|s|v] *paquete* o *código del producto*	La instalación con la opción /f reparará o reinstalará los archivos dañados o que falten. Por ejemplo, para forzar una reinstalación de todos los archivos, utilice la sintaxis siguiente: `msiexec /fa "C:\CarpetaWindows\Perfiles\NombreUsuario\Personal\MisValores\Othello\Versión de prueba\Release\ImágenesDisco\Disco1\Othello Beta.msi"` conjuntamente con los distintivos siguientes: • p reinstala un archivo si falta • o reinstala un archivo si falta o si está presente una versión más antigua del archivo en el sistema del usuario • e reinstala un archivo si falta o si un equivalente o una versión más antigua del archivo está presente en el sistema del usuario • c reinstala el archivo si falta o si la suma de comprobación almacenada del archivo instalado no coincide con el valor del nuevo archivo • a fuerza una reinstalación de todos los archivos • u o m regraba todas las entradas necesarias del registro del usuario • s sobregraba los accesos directos existentes • v ejecuta la aplicación a partir de las fuentes y vuelve a poner en la antememoria el paquete de instalación local
/a *paquete*	La opción /a permite a los usuarios con privilegios de administrador instalar un producto en la red.
/x *paquete* o *código del producto*	La opción /x desinstala un producto.
/L [i|w|e|a|r|u|c|m|p|v|+] *archivo de registro*	La creación de la opción /L especifica la vía de acceso del archivo de registro —estos distintivos indican la información que se almacenará en el archivo de registro: • i registra los mensajes de estado • w registra los mensajes de aviso no graves • e registra todos los mensajes de error • a registra el comienzo de las secuencias de acción • r registra registros específicos de la acción • u registra las solicitudes de usuario • c registra los parámetros iniciales de la interfaz de usuario • m registra los mensajes de memoria insuficiente • p registra los valores del terminal • v registra los valores de salida detallada • + se añade a un archivo existente • * es un carácter comodín que le permite registrar toda la información (excluido el valor de salida detallada)

Tabla 15. (continuación)

Parámetro	Descripción
/q [n|b|r|f]	La opción /q se utiliza para establecer el nivel de interfaz de usuario junto con los distintivos siguientes: • q o qn no crea ninguna interfaz de usuario • qb crea una interfaz básica de usuario Los siguientes valores de la interfaz de usuario visualizan un recuadro de diálogo modal al final de la instalación: • qr visualiza una interfaz de usuario reducida • qf visualiza una interfaz de usuario completa • qn+ no visualiza ninguna interfaz de usuario • qb+ visualiza una interfaz de usuario básica
/? o /h	Cualquiera de los dos mandatos visualiza la información de copyright de Windows Installer
TRANSFORMS	Utilice el parámetro de la línea de mandatos TRANSFORMS para especificar cualquier transformación que desee aplicar al paquete base. La llamada de la línea de mandatos de transformación tendrá un aspecto similar al siguiente: `msiexec /i "C:\CarpetaWindows\Perfiles\NombreUsuario\ Personal\MisValores\Nombre del proyecto\ Versión de prueba\Mi Release-1\ImágenesDisco\Disco1\ NombreProducto.msi" TRANSFORMS="New Transform 1.mst"` Puede separar varias transformaciones mediante un signo de punto y coma. Debido a esto, se recomienda que no utilice punto y coma en el nombre de la transformación, ya que el servicio de Windows Installer lo interpretará incorrectamente.
Propiedades	Todas las propiedades públicas se pueden establecer o modificar desde la línea de mandatos. Las propiedades públicas se distinguen de las propiedades privadas por el hecho de que están todas en mayúsculas. Por ejemplo, COMPANYNAME es una propiedad pública. Para establecer una propiedad en la línea de mandatos, utilice la sintaxis siguiente: PROPERTY=VALUE. Si deseara cambiar el valor de COMPANYNAME, especificaría lo siguiente: `msiexec /i "C:\CarpetaWindows\Perfiles\NombreUsuario\ Personal\MisValores\Nombre del proyecto\Versión de prueba\MiRelease-1\ImágenesDisco\Disco1\ NombreProducto.msi" COMPANYNAME="InstallShield"`

Propiedades públicas estándar de Windows Installer

Windows Installer tiene un conjunto de propiedades públicas estándar incorporadas que se pueden establecer en la línea de mandatos para especificar un comportamiento determinado durante la instalación. A continuación se describen las propiedades públicas más comunes utilizadas en la línea de mandatos. Existe más documentación disponible en el sitio Web de Microsoft en la dirección: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/about_properties.asp

La Tabla 16 muestra las propiedades más habitualmente utilizadas de Windows Installer:

Tabla 16.

Propiedad	Descripción
TARGETDIR	Especifica el directorio de destino raíz para la instalación. Durante una instalación administrativa, esta propiedad es la ubicación donde se debe copiar el paquete de instalación.
ARPAUTHORIZEDCDFPREFIX	URL del canal de actualización para la aplicación.
ARPCOMMENTS	Proporciona Comentarios para Agregar o quitar programas del Panel de control.
ARPCONTACT	Proporciona el Contacto para Agregar o quitar programas en el Panel de control.
ARPINSTALLLOCATION	Vía de acceso calificada totalmente de la carpeta primaria de la aplicación.
ARPNOMODIFY	Inhabilita la funcionalidad que modificaría el producto.
ARPNOREMOVE	Inhabilita la funcionalidad que eliminaría el producto.
ARPNOREPAIR	Inhabilita el botón Reparar del asistente de Programas.
ARPPRODUCTICON	Especifica el icono primario para el paquete de instalación.
ARPREADME	Proporciona un archivo ReadMe para Agregar o quitar programas en el Panel de control.
ARPSIZE	Tamaño aproximado de la aplicación en kilobytes.
ARPSYSTEMCOMPONENT	Evita que se visualice la aplicación en la lista de Agregar o quitar programas.
ARPURLINFOABOUT	URL de la página inicial de una aplicación.
ARPURLUPDATEINFO	URL de la información de actualización de la aplicación.
REBOOT	La propiedad REBOOT suprime algunos indicadores de solicitud para un rearranque del sistema. Un administrador utiliza normalmente este propiedad con una serie de instalaciones para instalar varios productos al mismo tiempo con sólo un rearranque al final. Establezca REBOOT=″R″ para inhabilitar el rearranque al final de una instalación.
INSTALLDIR	Esta propiedad contiene la carpeta de destino por omisión de los archivos en las características y los componentes.

Propiedades públicas de personalización de Rescue and Recovery

El paquete de instalación del programa Rescue and Recovery contiene un conjunto de propiedades públicas de personalización que se pueden establecer en la línea de mandato al ejecutar la instalación. Las propiedades públicas de personalización disponibles son las siguientes:

Tabla 17.

Propiedad	Descripción
PDA	Especifica si se debe instalar el Área previa al escritorio, el valor por omisión es 1. 1 = instalar Área previa al escritorio, 0 = no instalar Área previa al escritorio. NOTA: Este valor no se utiliza si si existe ya alguna versión del Área previa al escritorio.
CIMPROVIDER	Especifica si se debe instalar el componente del Proveedor CIM. El valor por omisión es no instalar el componente. Especifique CIMPROVIDER=1 en la línea de mandatos para instalar el componente.
EMULATIONMODE	Especifica que se fuerce la instalación en modalidad de emulación incluso si existe un TPM. Especifique EMULATIONMODE=1 en la línea de mandatos para instalar en modalidad de emulación.
HALTIFCSS54X	Si CSS 5.4X está instalado y la instalación se está ejecutando en modalidad silenciosa, el valor por omisión de la instalación es continuar en modalidad de emulación. Utilice la propiedad HALTIFCSS54X=1 al ejecutar la instalación en modalidad silenciosa para detener la instalación si CSS 5.4X está instalado.
HALTIFTPMDISABLED	Si TPM está en un estado inhabilitado y la instalación se está ejecutando en modalidad silenciosa, el valor por omisión es que la instalación continúe en modalidad de emulación. Utilice la propiedad HALTIFTPMDISABLED=1 al ejecutar la instalación en modalidad silenciosa para detener la instalación si TPM está inhabilitado.
ENABLETPM	Establezca ENABLETPM=0 en la línea de mandatos para impedir que la instalación habilite TPM.
NOCSS	Establezca NOCSS=1 en la línea de mandatos para impedir que se instalen Client Security Solution y sus subcaracterísticas. Esta propiedad está destinada a ser utilizada con una instalación silenciosa pero puede utilizarse también con una instalación UI. En la instalación UI, la característica CSS no se mostrará en la pantalla de instalación personalizada.

Tabla 17. (continuación)

Propiedad	Descripción
NOPRVDISK	Establezca NOPRVDISK=1 en la línea de mandatos para impedir que se instale la característica SafeGuard PrivateDisk. Esta propiedad está destinada a ser utilizada con una instalación silenciosa pero puede utilizarse también con una instalación UI. En la instalación UI, la característica SafeGuard PrivateDisk no se mostrará en la pantalla de instalación personalizada.
NOPWMANAGER	Establezca NOPWMANAGER=1 en la línea de mandatos para impedir que se instale la característica Password Manager. Esta propiedad está destinada a ser utilizada con una instalación silenciosa pero puede utilizarse también con una instalación UI. En la instalación UI, la característica Password Manager o se mostrará en la pantalla de instalación personalizada.
NOCSSWIZARD	Establezca NOCSSWIZARD=1 en la línea de mandatos para impedir que el Asistente de CSS se visualice cuando un usuario administrador inicie sesión y no se haya registrado. Esta propiedad está destinada a quienes deseen instalar CSS, pero utilicen posteriormente un script para configurar realmente el sistema.
CSS_CONFIG_SCRIPT	Establezca CSS_CONFIG_SCRIPT="*nombrearchivo*" o "*nombrearchivo contraseña*" para que se ejecute un archivo de configuración después de que el usuario haya completado la instalación y rearranque.
SUPERVISORPW	Establezca SUPERVISORPW="*contraseña*" en la línea de mandatos para proporcionar la contraseña de supervisor para habilitar el chip en modalidad de instalación silenciosa o no silenciosa. Si el chip está inhabilitado y la instalación se está ejecutando en modalidad silenciosa, se debe proporcionar la contraseña de supervisor correcta para habilitar el chip; de lo contrario, el chip no se habilitará.

Archivo de registro de instalación

Se crea un archivo de registro rrinstall30.log en el directorio %temp% si la instalación se ha iniciado mediante el archivo setup.exe (efectuando una doble pulsación en archivo exe principal de la instalación, ejecute el archivo exe principal de instalación sin parámetros o extraiga msi y ejecute setup.exe). Este archivo contiene mensajes de error que se pueden utilizar para solucionar problemas de instalación. Este archivo de registro no se crea al ejecutar la instalación directamente desde el paquete msi; esto incluye acciones realizadas desde Agregar o quitar programas. Para crear un archivo de registro para todas las acciones MSI, puede habilitar la política de registro en el registro. Para hacer esto, cree el valor:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer]
"Logging"="voicewarmup"
```

Ejemplos de instalación

La tabla siguiente muestra ejemplos que utilizan setup.exe:

Tabla 18.

Descripción	Ejemplo
Instalación silenciosa sin rearranque	`setup.exe /s /v"/qn REBOOT="R""`
Instalación administrativa	`setup.exe /a`
Instalación administrativa silenciosa especificando la ubicación de extracción	`setup.exe /a /s /v"/qn TARGETDIR="F:\TVTRR""`
Desinstalación silenciosa setup.exe /s /x /v/qn	`setup.exe /s /x /v/qn`
Instalación sin rearranque y creación de un registro de instalación en el directorio temporal	`setup.exe /v"REBOOT="R" /L*v %temp%\rrinstall30.log"`
Instalación sin la instalación del Área previa al escritorio setup.exe /vPDA=0	`setup.exe /vPDA=0`

La siguiente tabla muestra ejemplos de instalación que utilizan Rescue and Recovery/Client Security Solution.msi:

Tabla 19.

Descripción	Ejemplo
Instalación	msiexec /i "C:\TVTRR\Rescue and Recovery/Client Security Solution.msi"
Instalación silenciosa sin rearranque	msiexec /i "C:\TVTRR\Rescue and Recovery/Client Security Solution.msi" /qn REBOOT="R"
Instalación silenciosa	msiexec /x "C:\TVTRR\Rescue and Recovery/Client Security Solution.msi" /qn
Instalación sin la instalación del Área previa al escritorio	msiexec /i "C:\TVTRR\Rescue and Recovery/Client Security Solution.msi" PDA=0

Inclusión de Rescue and Recovery en una imagen de disco

Puede utilizar la herramienta que elija para crear una imagen del disco que incluya Rescue and Recovery. Esta guía de despliegue proporciona información básica relativa a PowerQuest y Ghost y a cómo se aplica a esta aplicación e instalación. Se asume que tiene experiencia con la herramienta de creación de imágenes y que incluirá otras opciones que necesita para las aplicaciones.

Nota: Si piensa crear una imagen, debe capturar el Registro de arranque maestro. El Registro de arranque maestro es crítico para que el entorno de Rescue and Recovery funcione correctamente.

Utilización de las herramientas basadas en imagen de la unidad de PowerQuest

Presuponiendo que la herramienta PowerQuest DeployCenter PQIMGCTR esté instalada en la siguiente ubicación (X:\PQ), puede crear y desplegar una imagen con Rescue and Recovery con los scripts siguientes:

Archivos de script mínimos

Tabla 20. X:\PQ\RRUSAVE.TXT

Idioma del script	Resultado
SELECT DRIVE 1	Selecciona la primera unidad de disco duro
SELECT PARTITION ALL (Necesario si tiene una partición de tipo 12 o si tiene múltiples particiones en la imagen.)	Selecciona todas las particiones
Almacena con compresión alta	Almacena la imagen

Tabla 21. X:\PQ\RRDEPLY.TXT

Idioma del script	Resultado
SELECT DRIVE 1	Selecciona la primera unidad de disco duro
DELETE ALL	Suprime todas las particiones
SELECT FREESPACE FIRST	Selecciona el primer espacio libre
SELECT IMAGE ALL	Selecciona todas las particiones de la imagen
RESTORE	Restaura la imagen

Creación de la imagen

Tabla 22. X:\PQ\PQIMGCTR / CMD=X:\PQ\RRUSAVE.TXT /MBI=1 / IMG=X:\IMAGE.PQI

Idioma del script	Resultado
SELECT DRIVE 1	Selecciona la primera unidad de disco duro
X:\PQ\PQIMGCTR	Programa de la imagen
/CMD=X:\PQ\RRUSAVE.TXT	Archivo script de PowerQuest
/MBI=1	Captura el Gestor de arranque de Rescue and Recovery
/IMG=X:\IMAGE.PQI	Archivo de imagen

Despliegue de la imagen

Tabla 23. X:\PQ\PQIMGCTR / CMD=X:\PQ\RRDEPLY.TXT /MBI=1 / IMG=X:\IMAGE.PQI

Idioma del script	Resultado
SELECT DRIVE 1	Selecciona la primera unidad de disco duro
X:\PQ\PQIMGCTR	Programa de la imagen
/CMD=X:\PQ\RRDEPLY.TXT	Archivo script de PowerQuest
/MBR=1	Restaura el Gestor de arranque de Rescue and Recovery
/IMG=X:\IMAGE.PQI	Archivo de imagen

Utilización de las herramientas basadas en Symantec Ghost

Cuando cree la imagen de Ghost, deberá utilizar el conmutador de la línea de mandatos (que puede estar incorporado en el archivo GHOST.INI) `-ib` para capturar el Gestor de arranque de Rescue and Recovery. Además, la imagen debe capturar todo el disco y todas las particiones. Consulte la documentación proporcionada por Symantec para obtener detalles específicos acerca de Ghost.

Componentes de instalación de Client Security Solution Versión 6.0

El paquete de instalación de Client Security Solution 6.0 se ha desarrollado con InstallShield 10.5 Premier como un proyecto MSI básico. Los proyectos MSI Básico de InstallShield 10.5 utilizan Windows Installer para instalar aplicaciones, lo que proporciona a los administradores muchas capacidades para personalizar instalaciones como por ejemplo establecer valores de propiedades desde la línea de mandatos. Las siguientes secciones describen formas de utilizar y ejecutar el paquete de instalación de CSS 6.0. Para una mejor comprensión, lea todas las instrucciones siguientes.

Componentes de la instalación

La instalación de CSS 6.0 consta de un único archivo exe (de aproximadamente 20 MB). Es el archivo setup.exe creado a partir de las fuentes del proyecto de instalación. El nombre del archivo setup.exe se cambia durante el proceso de creación a un nombre que representa el ID del proyecto, el tipo de soporte, el nivel de build, el código de país (siempre US en este caso) y el código de parche – por ejemplo, 169ZIS1001US00.exe. Se trata de un paquete de instalación autoextraíble que extrae los archivos fuente de la instalación e inicia la instalación utilizando Windows Installer. Contiene la lógica de la instalación y los archivos de las aplicaciones de Windows.

Procedimiento de instalación estándar y parámetros de la línea de mandatos

Setup.exe puede aceptar un conjunto de parámetros de la línea de mandatos, los cuales se describen a continuación. Las opciones de la línea de mandatos que requieren un parámetro se deben especificar sin ningún espacio entre la opción y su parámetro. Por ejemplo,

```
Setup.exe /s /v"/qn REBOOT="R""
```

es válido, mientras que

```
Setup.exe /s /v "/qn REBOOT="R""
```

no lo es. Es necesario que el parámetro de la opción esté entre comillas dobles sólo si el parámetro contiene espacios.

Nota: Por omisión, la instalación cuando se ejecuta sola (simplemente ejecutando setup.exe sin ningún parámetro) solicita al usuario que rearranque al final de la instalación. Es necesario rearrancar para que el programa funcione correctamente. Se puede aplazar el rearranque mediante un parámetro de la línea de mandatos para una instalación silenciosa, tal como se ha explicado anteriormente y en la sección de ejemplo.

Los parámetros y las descripciones siguientes se han tomado directamente de la documentación de ayuda del desarrollador de InstallShield. Se han eliminado los parámetros que no son aplicables a proyectos de MSI básico.

Tabla 24.

Parámetro	Descripción
/a : Instalación administrativa	El conmutador /a hace que setup.exe realice una instalación administrativa. Una instalación administrativa copia (y descomprime) los archivos de datos en un directorio especificado por el usuario, pero no crea atajos, registra servidores COM ni crea un registro de desinstalación.
/x : Modalidad de desinstalación	El conmutador /x hace que setup.exe desinstale un producto instalado anteriormente.
/s : Modalidad silenciosa	El mandato setup.exe /s suprime la ventana de inicialización de setup.exe para un programa de instalación MSI básico, pero no lee un archivo de respuestas. Los proyectos de MSI básico no crean ni utilizan un archivo de respuestas para las instalaciones silenciosas. Para ejecutar un producto de MSI básico de forma silenciosa, ejecute la línea de mandatos setup.exe /s /v/qn. (Para especificar los valores de las propiedades públicas para una instalación MSI básico, puede utilizar un mandato como por ejemplo setup.exe /s /v″/qn INSTALLDIR=D:\Destino″.)
/v : pasa argumentos a Msiexec	El argumento /v se utiliza para pasar conmutadores de la línea de mandatos y valores de propiedades públicas a Msiexec.exe.
/L : configura el idioma	Los usuarios pueden utilizar el conmutador /L con el ID decimal de idioma para especificar el idioma utilizado por el programa de instalación en varios idiomas. Por ejemplo, el mandato para especificar alemán es setup.exe /L1031. Nota: No todos los idiomas a los que se hace referencia en Tabla 25 están soportados en la instalación.
/w : Espera	Para un proyecto MSI básico, el argumento /w obliga a setup.exe a esperar hasta que se complete la instalación antes de salir. Si está utilizando la opción /w en un archivo de proceso por lotes, es posible que desee anteponer a todo el argumento de la línea del mandato setup.exe start /WAIT. A continuación se muestra un ejemplo correctamente formado de este uso: `start /WAIT setup.exe /w`

Tabla 25.

Idioma	Identificador
Árabe (Arabia Saudí)	1025
Vasco	1069
Búlgaro	1026

Tabla 25. (continuación)

Idioma	Identificador
Catalán	1027
Chino simplificado	2052
Chino tradicional	1028
Croata	1050
Checo	1029
Danés	1030
Holandés (estándar)	1043
Inglés	1033
Finlandés	1035
Francés de Canadá	3084
Francés	1036
Alemán	1031
Griego	1032
Hebreo	1037
Húngaro	1038
Indonesio	1057
Italiano	1040
Japonés	1041
Coreano	1042
Noruego (Bokmal)	1044
Polaco	1045
Portugués (Brasil)	1046
Portugués (estándar)	2070
Rumano	1048
Ruso	1049
Eslovaco	1051
Esloveno	1060
Español	1034
Sueco	1053
Tailandés	1054
Turco	1055

Procedimiento de instalación administrativo y parámetros de la línea de mandatos

Windows Installer puede realizar una instalación administrativa de una aplicación o de un producto en una red para que éste sea utilizado por un grupo de trabajo o para la personalización del mismo. Para el paquete de instalación de Rescue and Recovery/Client Security Solution, una instalación administrativa desempaqueta los archivos fuente de instalación en una ubicación específica. Para ejecutar una instalación administrativa es necesario ejecutar el paquete de instalación desde la línea de mandatos utilizando el parámetro /a:

```
Setup.exe /a
```

El inicio de la instalación administrativa presenta una serie de pantallas de diálogo que solicitan al usuario administrativo que especifique una ubicación donde desempaquetar los archivos de instalación. La ubicación de extracción por omisión que se presenta al usuario administrativo es C:\. Se puede seleccionar una nueva ubicación que puede incluir unidades que no sean la unidad C: (por ejemplo, otras unidades locales o unidades de red correlacionadas). También se pueden crear nuevos directorios durante este paso.

Si se ejecuta de forma silenciosa una instalación administrativa, se puede establecer en la línea de mandatos la propiedad pública TARGETDIR para que especifique la ubicación de extracción:

```
Setup.exe /s /v"/qn TARGETDIR=F:\TVTRR"
```

Una vez que se haya completado una instalación administrativa, el usuario administrativos puede realizar personalizaciones en los archivos fuente; por ejemplo, añadir valores adicionales a tvt.txt. Para instalar a partir de las fuentes desempaquetadas después de que se hayan realizado personalizaciones, el usuario llama a msiexec.exe desde la línea de mandatos, pasando el nombre del archivo msi desempaquetado. La sección siguiente describe los parámetros de la línea de mandatos disponibles que se pueden utilizar con msiexec, así como un ejemplo de cómo utilizarlos. Las propiedades públicas también se pueden establecer directamente en la llamada de la línea de mandatos de msiexec.

Parámetros de la línea de mandatos de msiExec.exe

MsiExec.exe es un programa ejecutable de Windows Installer utilizado para interpretar los paquetes de instalación e instalar productos en los sistemas de destino:

```
msiexec. /i "C:CarpetaWindows/Perfiles\NombreUsuario\Personal\MisValores\nombre
proyecto\configuración del producto\nombre de release\DiskImages\Disk1\nombre
del producto.msi
```

La tabla siguiente proporciona una descripción detallada de los parámetros de la línea de mandatos de MsiExec.exe. Esta tabla se toma directamente de la documentación de Microsoft Platform SDK de Windows Installer.

Tabla 26.

Parámetro	Descripción
/i *paquete* o *código del producto*	Utilice este formato para instalar el producto Othello: `msiexec /i "C:\CarpetaWindows\Perfiles\NombreUsuario\ Personal\MisConfiguraciones\Othello\Versión de prueba\Release\ImágenesDisco\Disco1\Othello Beta.msi"` El código del producto se refiere a la GUI que se genera automáticamente en la propiedad del Código del producto de la vista de proyectos del producto.

Tabla 26. (continuación)

Parámetro	Descripción
/f [p|o|e|d|c|a|u|m|s|v] *paquete* o *código del producto*	La instalación con la opción /f reparará o reinstalará los archivos dañados o que falten. Por ejemplo, para forzar una reinstalación de todos los archivos, utilice la sintaxis siguiente: `msiexec /fa "C:\CarpetaWindows\Perfiles\NombreUsuario \Personal\MisValores\Othello\Versión de prueba \Release\ImágenesDisco\Disco1\Othello Beta.msi"` conjuntamente con los distintivos siguientes: • p reinstala un archivo si falta • o reinstala un archivo si falta o si está presente una versión más antigua del archivo en el sistema del usuario • e reinstala un archivo si falta o si un equivalente o una versión más antigua del archivo está presente en el sistema del usuario • c reinstala el archivo si falta o si la suma de comprobación almacenada del archivo instalado no coincide con el valor del nuevo archivo • a fuerza una reinstalación de todos los archivos • u o m regraban todas las entradas necesarias del registro del usuario • s sobregraba los accesos directos existentes • v ejecuta la aplicación a partir de las fuentes y vuelve a poner en la antememoria el paquete de instalación local
/a *paquete*	La opción /a permite a los usuarios con privilegios de administrador instalar un producto en la red.
/x *paquete* o *código del producto*	La opción /x desinstala un producto.
/L [i|w|e|a|r|u|c|m|p|v|+] *archivo de registro*	La creación de la opción /L especifica la vía de acceso del archivo de registro —estos distintivos indican la información que se almacenará en el archivo de registro: • i registra los mensajes de estado • w registra los mensajes de aviso no graves • e registra todos los mensajes de error • a registra el comienzo de las secuencias de acción • r registra registros específicos de la acción • u registra las solicitudes de usuario • c registra los parámetros iniciales de la interfaz de usuario • m registra los mensajes de memoria insuficiente • p registra los valores del terminal • v registra los valores de salida detallada • + se añade a un archivo existente • * es un carácter comodín que le permite registrar toda la información (excluido el valor de salida detallada)

Tabla 26. (continuación)

Parámetro	Descripción
/q [n|b|r|f]	La opción /q se utiliza para establecer el nivel de interfaz de usuario junto con los distintivos siguientes: • q o qn no crea ninguna interfaz de usuario • qb crea una interfaz básica de usuario Los siguientes valores de la interfaz de usuario visualizan un recuadro de diálogo modal al final de la instalación: • qr visualiza una interfaz de usuario reducida • qf visualiza una interfaz de usuario completa • qn+ no visualiza ninguna interfaz de usuario • qb+ visualiza una interfaz de usuario básica
/? o /h	Cualquiera de los dos mandatos visualiza la información de copyright de Windows Installer
TRANSFORMS	Utilice el parámetro de la línea de mandatos TRANSFORMS para especificar cualquier transformación que desee aplicar al paquete base. La llamada de la línea de mandatos a la transformación puede tener un aspecto similar al siguiente: `msiexec /i "C:\CarpetaWindows\Perfiles\NombreUsuario\ Personal\MisValores\Nombre del proyecto\Versión de prueba\MiRelease-1\ImágenesDisco\Disco1\ NombreProducto.msi" TRANSFORMS="Nueva transformación 1.mst"` Puede separar varias transformaciones mediante un signo de punto y coma. Debido a esto, se recomienda que no utilice punto y coma en el nombre de la transformación, ya que el servicio de Windows Installer lo interpretará incorrectamente.
Propiedades	Todas las propiedades públicas se pueden establecer o modificar desde la línea de mandatos. Las propiedades públicas se distinguen de las propiedades privadas por el hecho de que están todas en mayúsculas. Por ejemplo, COMPANYNAME es una propiedad pública. Para establecer una propiedad en la línea de mandatos, utilice la sintaxis siguiente: PROPERTY=VALUE. Si deseara cambiar el valor de COMPANYNAME, especificaría lo siguiente: `msiexec /i "C:\CarpetaWindows\Perfiles\NombreUsuario \Personal\MisValores\Nombre del proyecto\Versión de prueba\Mi Release-1\ImágenesDisco\Disco1\NombreProducto.msi" COMPANYNAME="InstallShield"`

Propiedades públicas estándar de Windows Installer

Windows Installer tiene un conjunto de propiedades públicas estándar incorporadas que se pueden establecer en la línea de mandatos para especificar un comportamiento determinado durante la instalación. A continuación se describen las propiedades públicas más comunes utilizadas en la línea de mandatos. Existe más documentación disponible en el sitio Web de Microsoft en la dirección: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/about_properties.asp

La tabla 3 muestra las propiedades más habitualmente utilizadas de Windows Installer:

Tabla 27.

Propiedad	Descripción
TARGETDIR	Especifica el directorio de destino raíz para la instalación. Durante una instalación administrativa, esta propiedad es la ubicación donde se debe copiar el paquete de instalación.
ARPAUTHORIZEDCDFPREFIX	URL del canal de actualización para la aplicación.
ARPCOMMENTS	Propporciona Comentarios para Agregar o quitar programas del Panel de control.
ARPCONTACT	Proporciona el Contacto para Agregar o quitar programas en el Panel de control.
ARPINSTALLLOCATION	Vía de acceso calificada totalmente de la carpeta primaria de la aplicación.
ARPNOMODIFY	Inhabilita la funcionalidad que modificaría el producto.
ARPNOREMOVE	Inhabilita la funcionalidad que eliminaría el producto.
ARPNOREPAIR	Inhabilita el botón Reparar del asistente de Programas.
ARPPRODUCTICON	Especifica el icono primario para el paquete de instalación.
ARPREADME	Proporciona un archivo ReadMe para Agregar o quitar programas en el Panel de control.
ARPSIZE	Tamaño aproximado de la aplicación en kilobytes.
ARPSYSTEMCOMPONENT	Evita que se visualice la aplicación en la lista de Agregar o quitar programas.
ARPURLINFOABOUT	URL de la página inicial de una aplicación.
ARPURLUPDATEINFO	URL de la información de actualización de la aplicación.
REBOOT	La propiedad REBOOT suprime algunos indicadores de solicitud para un rearranque del sistema. Un administrador utiliza normalmente este propiedad con una serie de instalaciones para instalar varios productos al mismo tiempo con sólo un rearranque al final. Establezca REBOOT=”R” para inhabilitar el rearranque al final de una instalación.
INSTALLDIR	Esta propiedad contiene la carpeta de destino por omisión de los archivos en las características y los componentes.

Propiedades públicas de personalización de Client Security Software

El paquete de instalación del programa Client Security Software contiene un conjunto de propiedades públicas de personalización que se pueden establecer en la línea de mandatos al ejecutar la instalación. Las propiedades públicas de personalización disponibles son las siguientes:

Tabla 28.

Propiedad	Descripción
EMULATIONMODE	Especifica que se fuerce la instalación en modalidad de emulación incluso si existe un TPM. Especifique EMULATIONMODE=1 en la línea de mandatos para instalar en modalidad de emulación.
HALTIFTPMDISABLED	Si TPM está en un estado inhabilitado y la instalación se está ejecutando en modalidad silenciosa, el valor por omisión es que la instalación continúe en modalidad de emulación. Utilice la propiedad HALTIFTPMDISABLED=1 al ejecutar la instalación en modalidad silenciosa para detener la instalación si TPM está inhabilitado.
ENABLETPM	Establezca ENABLETPM=0 en la línea de mandatos para impedir que la instalación habilite TPM.
NOPRVDISK	Establezca NOPRVDISK=1 en la línea de mandatos para impedir que se instale la característica SafeGuard PrivateDisk. Esta propiedad está destinada a ser utilizada con una instalación silenciosa pero puede utilizarse también con una instalación UI. En la instalación UI, la característica SafeGuard PrivateDisk no se mostrará en la pantalla de instalación personalizada.
NOPWMANAGER	Establezca NOPWMANAGER=1 en la línea de mandatos para impedir que se instale la característica Password Manager. Esta propiedad está destinada a ser utilizada con una instalación silenciosa pero puede utilizarse también con una instalación UI. En la instalación UI, la característica Password Manager o se mostrará en la pantalla de instalación personalizada.
NOCSSWIZARD	Establezca NOCSSWIZARD=1 en la línea de mandatos para impedir que el Asistente de CSS se visualice cuando un usuario administrador inicie sesión y no se haya registrado. Esta propiedad está destinada a quienes deseen instalar CSS, pero utilicen posteriormente un script para configurar realmente el sistema.

Tabla 28. (continuación)

Propiedad	Descripción
CSS_CONFIG_SCRIPT	Establezca CSS_CONFIG_SCRIPT="*nombrearchivo*" o "*nombrearchivo contraseña*" para que se ejecute un archivo de configuración después de que el usuario haya completado la instalación y rearranque.
SUPERVISORPW	Establezca SUPERVISORPW="*contraseña*" en la línea de mandatos para proporcionar la contraseña de supervisor para habilitar el chip en modalidad de instalación silenciosa o no silenciosa. Si el chip está inhabilitado y la instalación se está ejecutando en modalidad silenciosa, se debe proporcionar la contraseña de supervisor correcta para habilitar el chip; de lo contrario, el chip no se habilitará.

Archivo de registro de instalación

Se crea un archivo de registro cssinstall60.log en el directorio %temp% si la instalación se ha iniciado mediante el archivo setup.exe (efectuando una doble pulsación en el archivo exe principal de la instalación, ejecute el archivo exe principal sin parámetros o extraiga msi y ejecute setup.exe). Este archivo contiene mensajes de error que se pueden utilizar para solucionar problemas de instalación. Este archivo de registro no se crea al ejecutar la instalación directamente desde el paquete msi, esto incluye algunas acciones realizadas desde Agregar o quitar programas. Para crear un archivo de registro para todas las acciones MSI, puede habilitar la política de registro en el registro. Para hacer esto, cree el valor:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer]
"Logging"="voicewarmup"
```

Ejemplos de instalación

La tabla siguiente muestra ejemplos que utilizan setup.exe:

Tabla 29.

Descripción	Ejemplo
Instalación silenciosa sin rearranque	`setup.exe /s /v"/qn REBOOT="R""`
Instalación administrativa	`setup.exe /a`
Instalación administrativa silenciosa especificando la ubicación de extracción	`setup.exe /a /s /v"/qn TARGETDIR="F:\CSS60""`
Desinstalación silenciosa setup.exe /s /x /v/qn	`setup.exe /s /x /v/qn`
Instalación sin rearranque y creación de un registro de instalación en el directorio temporal	`setup.exe /v"REBOOT="R" /L*v %temp%\cssinstall60.log"`
Instalación sin la instalación del Área previa al escritorio setup.exe /vPDA=0	`setup.exe /vPDA=0`

La tabla siguiente muestra los ejemplos de instalación utilizando Client Security Solution.msi:

Tabla 30.

Descripción	Ejemplo
Instalación	`msiexec /i "C:\CSS60\Client Security Solution.msi"`
Instalación silenciosa sin rearranque	`msiexec /i "C:\CSS60\Client Security Solution.msi" /qn REBOOT="R"`
Instalación silenciosa	`msiexec /x "C:\CSS60\Client Security Solution.msi" /qn`

Instalación de System Migration Assistant

El procedimiento de instalación de System Migration Assistant se documenta en el manual *System Migration Assistant Guía del usuario*.

Instalación del Software de huellas dactilares

El archivo setup.exe del programa Software de huellas dactilares se puede iniciar con los parámetros siguientes:

Instalación silenciosa

También está disponible la instalación silenciosa del Software de huellas dactilares. Ejecute Setup.exe en el directorio de instalación de la unidad de CD-ROM.

Utilice la sintaxis siguiente:

`Setup.exe` *`PROPERTY=VALUE`* `/q /i`

donde *q* es para la instalación silenciosa y *i* es para la instalación. Por ejemplo:

```
Setup.exe INSTALLDIR="F:\Archivos de programa\IBM fingerprint software" /q /i
```

Para desinstalar el software, utilice en su lugar el parámetro /x:

```
Setup.exe INSTALLDIR="F:\Archivos de programa\IBM fingerprint software" /q /x
```

Instalación de SMS

También están permitidas las instalaciones de SMS. Abra la Consola del administrador de SMS, cree un nuevo paquete y establezca las propiedades del paquete de la forma estándar. Abra el paquete y seleccione Nuevo-Programa en el elemento Programas. En la línea de mandatos, especifique:

`Setup.exe /m` *`nombrearchivomif`* `/q /i`

Puede utilizar los mismos parámetros para la instalación silenciosa.

La instalación normalmente rearranca al final del proceso de instalación. Si desea suprimir todos los rearranques durante la instalación y rearrancar posteriormente (después de instalar más programas), añada REBOOT=″ReallySuppress″ a la lista de propiedades.

Opciones

En el Software de huellas dactilares están soportadas las opciones siguientes:

Tabla 31.

Parámetro	Descripción
CTRLONCE	Utilizado para visualizar sólo una vez el Centro de control. El valor por omisión es 0.
CTLCNTR	Utilizado para ejecutar el Centro de control al arrancar. El valor por omisión es 1.
DEFFUS	#0 instala nuestro inicio de sesión, no se preocupa de los valores de FUS. (valor por omisión para primeras instalaciones, en Reparar/Modificar/Actualizar establecido en 1 si FUS está activo) #1 detecta los valores de FUS del sistema y los intenta mantener.
INSTALLDIR	Directorio de instalación por omisión del Software de huellas dactilares
OEM	• 0 = Instala soporte para pasaportes de servidor/autentificación de servidor • 1 = Sólo modalidad autónoma del sistema con pasaportes locales
PASSPORT	Tipo de pasaporte por omisión establecido durante la instalación. • 1 = Valor por omisión - Pasaporte local • 2 = Pasaporte del servidor El valor por omisión es 1.
SECURITY	• 1 - = Instala soporte para la modalidad segura • 0 = No instala; sólo existe la modalidad cómoda
SHORTCUTFOLDER	Nombre por omisión de la carpeta de acceso directo en el menú Inicio
REBOOT	Se puede utilizar para suprimir todos los rearranques incluidos los indicadores de solicitud durante la instalación estableciéndolo en ReallySuppress.

Escenarios de software instalado

Tabla 32.

Software instalado	Notas
Client Security Software Versión 5.4x	Es la única versión de CSS que puede coexistir con Rescue and Recovery.

Tabla 32. (continuación)

Software instalado	Notas
Rescue and Recovery Versión 3.0 solamente	• Se instala mediante la instalación completa del producto, con CSS deseleccionado. • Algunos componentes principales de Client Security Solution se instalan en la instalación de sólo RnR para permitir el cifrado de las copias de seguridad con TMP, y para la configuración de la contraseña maestra de PDA.
Client Security Solution Versión 6.0 autónomo	• Es un paquete de instalación separado • No puede instalar todo el producto y deseleccionar Rescue and Recovery para obtener sólo Client Security Solution • Los componentes de CSS (Private Disk y Password Manager) son opcionales.
Rescue and Recovery Versión 3.0 y Client Security Solution Versión 6.0	• Precarga por omisión - Se instala mediante la instalación normal del producto • Componentes de CSS • Private Disk y Password Manager son componentes opcionales

Modificación del estado del software

Tabla 33.

Si el software instalado es....	Y desea cambiarlo a.....	Siga este proceso.....	Notas	Build
Client Security Software Versión 5.4x	Client Security Software 5.4x y Rescue and Recovery Versión 3.0	• Instale el producto. • Sólo se instalarán los componentes de Rescue and Recovery (no se visualizará ninguna pantalla de configuración). • Cuando se le solicite, indique que desea mantener instalado Client Security Software.	• Client Security Software comprueba que Rescue and Recovery se haya implementado utilizando la modalidad de emulación • En esta modalidad sólo está disponible la contraseña maestra mediante Client Security Software.	011
Client Security Software	Client Security Solution 6.0	• Desinstale Client Security Software 5.4x • Instale Client Security Solution 6.0 autónomo	No está permitido intentar instalar Client Security Solution Versión 6.0 encima de Client Security Software Versión 5.4x. Se solicita primero al usuario que elimine el Client Security Software antiguo	011

Tabla 33. (continuación)

Si el software instalado es....	Y desea cambiarlo a.....	Siga este proceso.....	Notas	Build
Client Security Software	Rescue and Recovery Versión 3.0 y Client Security Solution Versión 6.0	• Desinstale Client Security Software 5.4x • Instale el producto.	Si se intenta instalar el producto encima de Client Security Software Versión 5.4x se le preguntará si desea eliminar primero Client Security Software Versión 5.4x. Si la instalación continúa sin la desinstalación, sólo se instalará Rescue and Recovery.	011

Tabla 34.

Si el software instalado es....	Y desea cambiarlo a.....	Siga este proceso.....	Notas	Build
Rescue and Recovery Versión 3.0	Client Security Software 5.4x y Rescue and Recovery Versión 3.0	• Desinstale Rescue and Recovery • Instale Client Security Software Versión 5.4x • Instale el producto de la forma descrita anteriormente	• Client Security Software Versión 5.4x no se puede instalar encima de otra instalación del producto. • Las copias de seguridad locales se suprimen durante la desinstalación de Rescue and Recovery Versión 3.0	011
Rescue and Recovery Versión 3.0	Client Security Solution 6.0	• Desinstale Rescue and Recovery Versión 3.0 • Instale Client Security Solution Versión 6.0 autónomo	• La desinstalación de Rescue and Recovery Versión 3.0 suprimirá los archivos de usuario y los valores de registro de CSS. • Las copias de seguridad de Rescue and Recovery Versión 3.0 protegidas mediante CSS dejarán de ser accesibles. • Las copias de seguridad locales se suprimen durante la desinstalación de Rescue and Recovery Versión 3.0. • La instalación de Client Security Software Versión 6.0 autónomo no está permitida encima de otra instalación del producto. • La opción 'Modificar' de Agregar o quitar programas sólo permitirá la adición de Client Security Solution en este caso. Rescue and Recovery no se puede eliminar mediante la opción 'Modificar'.	012

Tabla 34. (continuación)

Si el software instalado es....	Y desea cambiarlo a.....	Siga este proceso.....	Notas	Build
Rescue and Recovery Versión 3.0	Rescue and Recovery Versión 3.0 y Client Security Solution Versión 6.0	• Seleccione la opción 'Modificar' de Agregar o quitar programas. • Añada CSS y los componentes adicionales.	• Las copias de seguridad locales se suprimen al añadir CSS. • Al añadir Client Security Solution se avisará al usuario de que debe realizar nuevas copias de seguridad después de añadir Client Security Solution. • Cuando se añade Client Security Solution se borran los valores y los archivos de datos de Client Security Solution. • No está permitida la instalación de Client Security Solution Versión 6.0 sobre otra instalación del producto.	A determinar

Tabla 35.

Si el software instalado es....	Y desea cambiarlo a.....	Siga este proceso.....	Notas	Build
Client Security Solution Versión 6.0 autónomo	Client Security Software 5.4x	• Desinstale Client Security Solution Versión 6.0 • Instale Client Security Software Versión 5.4x	• No se puede instalar Client Security Solution Versión 5.4x sobre otra instalación del producto. • La desinstalación de Client Security Solution Versión 6.0 solicitará la desinstalación de los archivos de datos y los valores. La opción seleccionada aquí no afecta de ninguna manera al funcionamiento de Client Security Software Versión 5.4x.	011

Tabla 35. (continuación)

Si el software instalado es....	Y desea cambiarlo a.....	Siga este proceso.....	Notas	Build
Client Security Solution Versión 6.0 autónoma	Rescue and Recovery Versión 3.0	• Desinstale Client Security Solution Versión 6.0 • Instale el producto y seleccione solamente Rescue and Recovery	• La desinstalación de Client Security Solution Versión 6.0 le preguntará sobre si deben suprimirse los archivos de usuario y los valores de Client Security Solution Versión 6.0. • La instalación de Rescue and Recovery 3.0 solicitará al usuario que elimine los archivos de usuario y los valores existentes de Client Security Solution. Si el usuario selecciona no eliminar los archivos, la instalación se cancelará.	012

Tabla 35. (continuación)

Si el software instalado es....	Y desea cambiarlo a.....	Siga este proceso.....	Notas	Build
Client Security Solution Versión 6.0 autónoma	Rescue and Recovery Versión 3.0 y Client Security Solution Versión 6.0	• Ejecute la instalación del producto • No se pueden deseleccionar las opciones de Rescue and Recovery y Client Security Solution • Los componentes instalados de Client Security Solution (Password Manager y Private Disk) están seleccionados por omisión, pero se pueden deseleccionar. Los componentes que no se han instalado anteriormente estarán deseleccio-nados por omisión, pero se pueden seleccionar.	• Client Security Solution Versión 6.0 autónoma se desinstalará en segundo plano. • Los archivos de datos y los valores de Client Security Solution Versión 6.0 se conservarán. • El estado de emulación/no emulación se conservará. • Después de que se haya completado la instalación del producto, el Asistente de Client Security Solution no se ejecutará porque Client Security Solution se ha configurado anteriormente. • La opción de proteger las copias de seguridad de Rescue and Recovery con Client Security Solution se debe realizar mediante la GUI de Rescue and Recovery. Existirá la opción de ejecutar la GUI de Rescue and Recovery después de rearrancar en la última pantalla de la instalación. • Después de instalar el producto, las opciones de Agregar o quitar programas incluirán 'Eliminar', 'Reparar' y 'Modificar'. • La versión instalada de Client Security Solution Versión 6.0 debe ser igual o inferior a la versión del producto que se está instalando; de lo contrario, el usuario visualizará un mensaje que le indicará que el producto no se puede instalar.	012

Notas:

1. Si el usuario instala Rescue and Recovery 3.0 de forma silenciosa, los archivos de usuario y los valores de Client Security Solution se suprimirán automáticamente durante la instalación.
2. En este escenario, la selección o deselección de Password Manager y de Private Disk durante la instalación del producto (Rescue and Recovery 3.0 y Client Security Solution 6.0) determina el estado final del componente después de la instalación del producto. Por ejemplo, si se ha instalado Password Manager con Client Security Solution 6.0 y el usuario lo deselecciona durante la instalación del producto, ya no se instalará después de que se complete la instalación. Si se ejecuta la instalación del producto (Rescue and Recovery y Client Security Solution) de forma silenciosa, tanto Password Manager como Private Disk se instalarán a menos que las propiedades respectivas NOPRVDISK=1 o NOPWMANAGER=1 estén establecidas en el mandato de instalación.

Tabla 36.

Si el software instalado es....	**Y desea cambiarlo a.....**	**Siga este proceso.....**	**Notas**	**Build**
Rescue and Recovery Versión 3.0 y Client Security Solution Versión 6.0	Client Security Software 5.4x	• Desinstale el producto • Instale Client Security Solution Versión 5.4x	• Client Security Software Versión 5.4x no se puede instalar encima de otra instalación del producto. • La desinstalación del producto solicitará la supresión de los archivos de datos y los valores. La opción seleccionada aquí no afecta de ninguna manera al funcionamiento de Client Security Software Versión 5.4x.	011
Rescue and Recovery Versión 3.0 y Client Security Solution Versión 6.0	Rescue and Recovery Versión 3.0	• Seleccione la opción 'Modificar' de Agregar o quitar programas. • Elimine Client Security Solution.	• Las copias de seguridad locales se suprimen cuando se suprime Client Security Solution. • La desinstalación de Client Security Solution avisará sobre la pérdida de PrivateDisk y Password Manager. • Las copias de seguridad de Rescue and Recovery Versión 3.0 protegidas mediante Client Security Solution dejarán de ser accesibles. • Los valores y los archivos de datos de Client Security Solution se suprimirán cuando se elimine Client Security Solution de 'Modificar'.	A determinar. No en el Build 12

Tabla 36. (continuación)

Si el software instalado es....	Y desea cambiarlo a.....	Siga este proceso.....	Notas	Build
Rescue and Recovery Versión 3.0 y Client Security Solution Versión 6.0	Client Security Solution Versión 6.0	• Desinstale el producto. • La desinstalación solicitará la supresión de los archivos y los valores de Client Security Solution. Se pueden conservar si el usuario desea mantener la configuración existente de Client Security Solution. • Instale Client Security Solution Versión 6.0 autónoma	• Desinstale el producto. • La desinstalación solicitará la supresión de los archivos y los valores de Client Security Solution. Se pueden conservar si el usuario desea mantener la configuración existente de Client Security Solution. • Instale Client Security Solution Versión 6.0 autónoma	012

Notas:

1. Durante una desinstalación de Client Security Solution 6.0 desde Agregar o quitar programas o una desinstalación desde la interfaz de usuario de la fuente original, se solicitará al usuario que suprima los valores y los archivos de datos de CSS. Si la desinstalación se ejecuta de forma silenciosa desde la línea de mandatos, el valor por omisión es suprimir los valores y los archivos de datos de CSS; sin embargo, este acción se puede modificar temporalmente estableciendo la propiedad NOCSSCLEANUP=1 en el mandato de desinstalación.
2. Durante la desinstalación del producto (Rescue and Recovery y Client Security Solution 6.0) desde Agregar o quitar programas o durante una desinstalación desde la interfaz de usuario de la fuente original, se solicitará al usuario que suprima los valores y los archivos de datos de Client Security Solution. Si la desinstalación se ejecuta de forma silenciosa desde la línea de mandatos, el valor por omisión es suprimir los valores y los archivos de datos de Client Security Solution; sin embargo, esta acción se puede modificar temporalmente estableciendo la propiedad NOCSSCLEANUP=1 en el mandato de desinstalación.

Capítulo 7. Infraestructura de Antidote Delivery Manager

Antidote Delivery Manager funciona entregando instrucciones de un administrador a cada sistema y dando soporte a mandatos para combatir un virus o un gusano. El administrador prepara un script que contiene las acciones deseadas en cada sistema. La función depósito entrega el script de forma segura al sistema en cuestión de minutos y ejecuta los mandatos. Los mandatos incluyen la restricción de las conexiones de red, la visualización de mensajes a los usuarios finales, la restauración de archivos desde copias de seguridad, la descarga de archivos, la ejecución de otros mandatos del sistema y el reinicio de la máquina en el mismo sistema operativo, o bien entrar o salir del entorno de Rescue and Recovery. Tanto la función depósito como los mandatos funcionan tanto en el sistema operativo normal (por ejemplo, Windows XP) o en el entorno Rescue and Recovery.

La estrategia global para combatir un virus consiste en reducir la expansión y el daño del código maligno, aplicar parches y realizar la limpieza en cada sistema y, a continuación, poner las máquinas restauradas de nuevo en la red. En el caso de un virus altamente destructivo y con una rápida expansión, es posible que sea necesario quitar sistemas de la red y realizar todas las reparaciones en el entorno de Rescue and Recovery. Aunque éste es el método más seguro, también causa interrupciones a los usuarios finales si se aplica durante las horas habituales de trabajo. En algunas circunstancias, se puede postergar o evitar la conmutación al entorno de Rescue and Recovery restringiendo las capacidades de red. El paso siguiente es descargar los parches y el código de limpieza, ejecutar el código de limpieza e instalar los parches para la instalación. En general, los parches están diseñados para ser instalados mientras el sistema operativo se está ejecutando, pero es posible que sea más adecuado realizar la limpieza y otras operaciones en el entorno de Rescue and Recovery. Cuando se hayan completado las operaciones correctoras, se podrá restaurar el funcionamiento normal del sistema con Windows XP en ejecución y las configuraciones de red restauradas.

Las dos secciones siguientes describen detalladamente el funcionamiento y los mandatos de depósito. A continuación, se presentan la instalación y la configuración de la función. Las secciones siguientes son ejemplos de cómo utilizar el sistema para las tareas habituales de comprobación, respuesta a virus destructivos, de dirigirse a máquinas conectadas mediante redes inalámbricas o VPN (Virtual Private Networks) y de solución de problemas que causen menos daño.

Depósito

La función de depósito se ejecuta en cada sistema y comprueba periódicamente si hay nuevos mensajes del administrador. Realiza la comprobación en un intervalo de tiempo planificado o cuando se producen varios sucesos destacados (por ejemplo, el arranque, la reanudación desde la suspensión o hibernación, la detección de un nuevo adaptador de red y la asignación de una nueva dirección IP). La función de depósito busca los mensajes en una serie de directorios, en una ubicación de compartición Windows, por ejemplo, \\máquina\compartición\directorio, en URL HTTP y en URL FTP. Si se encuentra más de un mensaje, los procesa en el orden “clasificación de directorios por nombre”. Sólo se procesa un mensaje cada vez. Un mensaje se procesa

satisfactoriamente sólo una vez. Si el proceso de un mensaje falla, por ejemplo, no se vuelve a intentar, pero se puede especificar en el propio mensaje que se vuelva a intentar después de un fallo.

Un administrador debe empaquetar un mensaje antes de colocarlo en un directorio para que sea procesado por la función depósito. Para crear el paquete, el administrador coloca todos los archivos que constituyen el mensaje en un directorio (o sus subdirectorios). Uno de los archivos se debe denominar "GO.RRS", el script de mandatos primario. El administrador puede utilizar opcionalmente una clave de firma para este mensaje, pero si se utiliza la clave debe estar disponible para todos los sistemas de destino. La función depósito comprueba la integridad del paquete, comprueba la firma, si se proporciona, y desempaqueta todos los archivos en un directorio local antes de ejecutar GO.RRS.

El archivo del script de mandatos primario (GO.RRS) sigue la sintaxis del archivo de mandatos de Windows. Es posible que contenga mandatos legítimos de Windows y cualquiera de los mandatos listados en la sección siguiente. Además, también se instala un intérprete de mandatos Python como parte del entorno de Rescue and Recovery, por lo que desde el script GO.RRS también se puede llamar a scripts de Python.

Al final de la ejecución del script, todos los archivos desempaquetados del mensaje se suprimen, así que si se necesitan archivos después de salir del script (por ejemplo, instalando un parche al rearrancar), todos los archivos se deben sacar del directorio de mensajes.

Cada sistema tiene una configuración de depósitos para comprobar. Es posible que sea adecuado que el administrador de TI divida el conjunto de sistemas en grupos y que asigne distintos depósitos (comparticiones de red) a cada grupo. Por ejemplo, se pueden agrupar los sistemas geográficamente según la proximidad al servidor de archivos. O bien se pueden agrupar los sistemas por función, por ejemplo, técnicos, ventas o soporte.

Mandatos de Antidote Delivery Manager y mandatos de Windows disponibles

El sistema Antidote Delivery Manager proporciona varios mandatos para facilitar el manejo del sistema. Además de los mandatos para crear mensajes y ajustar valores, existen mandatos para controlar las comunicaciones de red, determinar y controlar el estado operativo del sistema, examinar los archivos XML de los inventarios del sistema y notificar al usuario final del progreso del script de Antidote Delivery Manager en la máquina cliente. El mandato NETWK habilita o inhabilita las comunicaciones de red o las restringe a un grupo limitado de direcciones de la red. El mandato INRR se puede utilizar para determinar si el sistema operativo Windows XP está en ejecución o si el sistema está en el entorno de Rescue and Recovery. El mandato REBOOT se puede utilizar para concluir el sistema y especificar que se debe arrancar en Windows XP o bien en Rescue and Recovery. La aplicación MSGBOX permite la comunicación con el usuario final visualizando un mensaje en un recuadro emergente. El recuadro de mensaje puede contener opcionalmente los botones Aceptar y Cancelar de forma que el mensaje puede resultar en un comportamiento diferente según lo que especifique el usuario.

Algunos mandatos de Microsoft están también disponibles para Antidote Delivery Manager. Los mandatos permitidos incluyen todos los mandatos incorporados en

el shell de mandatos, por ejemplo, DIR o CD. Están disponibles otros mandatos útiles, como por ejemplo REG.EXE para cambiar el registro y CHKDSK.EXE para verificar la integridad del disco.

Utilización típica de Antidote Delivery Manager

El sistema Antidote Delivery Manager se puede utilizar para completar una gran variedad de tareas. Los ejemplos siguientes muestran cómo es posible utilizar el sistema.

- **Prueba simple del sistema - Visualizar notificación**

  La utilización más básica del sistema es visualizar un único mensaje al usuario final. La forma más sencilla de ejecutar esta prueba y también de probar otros scripts antes de su despliegue es colocar el mensaje en un depósito, que es un directorio local del PC del administrador. Esta colocación permite la comprobación rápida del script sin que afecte a otras máquinas.

- **Preparación y empaquetado del script**

  Grabe un script GO.RRS en cualquier otra máquina donde se haya instalado Antidote Delivery Manager. Incluya una línea como la siguiente: `MSGBOX /MSG "Hola gente" /OK`. Para crear un mensaje, ejecute el mandato APKGMSG en el directorio que contiene GO.RRS.

- **Ejecución del script**

  Coloque el archivo del mensaje en uno de los directorios del depósito de la máquina y vigile un correcto funcionamiento. Cuando a continuación se ejecute el agente de correo, se visualizará un recuadro de mensaje con el texto “Hola gente”. Dicho script es también una buena manera de comprobar depósitos de red y de demostrar funciones como por ejemplo la comprobación de los depósitos al reanudar después de la modalidad de suspensión.

Ataque importante de gusanos

El ejemplo muestra un posible procedimiento para combatir un virus importante. El procedimiento básico es desactivar las comunicaciones de red y, a continuación, rearrancar en Rescue and Recovery, recuperar los arreglos, realizar las reparaciones y, a continuación, arrancar de nuevo en Windows XP, instalar los parches y, finalmente, restaurar las comunicaciones de red. Se puede utilizar un único mensaje para realizar todas estas funciones mediante la utilización de archivos de distintivos y el mandato RETRYONERROR.

1. **Fase de bloqueo**

   La primera acción que se debe realizar es informar al usuario final de lo que va a suceder. Si el ataque no es extremadamente grave, el administrador puede dar al usuario final la opción de postergar el arreglo para más tarde. Lo más prudente sería utilizar esta fase para inhabilitar las comunicaciones de red y proporcionar un breve período de tiempo de unos 15 minutos en el que el usuario final pudiera guardar el trabajo que estuviera realizando. RETRYONERROR se utiliza para mantener el script en ejecución y, a continuación, se puede rearrancar la máquina en el entorno de Rescue and Recovery.

2. **Fase de distribución del código y fase de reparación**

   Ahora que ha desaparecido la amenaza de infección inhabilitando la red y rearrancando en Rescue and Recovery, se puede recuperar código adicional y realizar las reparaciones. Se puede habilitar la red o bien se pueden permitir algunas direcciones durante el tiempo necesario para recuperar los archivos adicionales. Mientras está en Rescue and Recovery, se pueden eliminar los archivos de virus y el registro se puede borrar. Desgraciadamente, no es posible

la instalación de nuevo software o parches porque los parches presuponen que se está ejecutando Windows XP. Con las comunicaciones de red aún inhabilitadas y todos los virus eliminados, es seguro rearrancar en Windows XP para completar las reparaciones. Un archivo de etiqueta grabado en este momento redirige al script a la sección de parches después del rearranque.

3. **Fase de parche y recuperación**

   Cuando la máquina se rearranca en Windows XP, Antidote Delivery Manager empieza a procesarse de nuevo incluso antes de que el usuario final inicie la sesión. En este momento se deben instalar los parches. La máquina se puede rearrancar una vez más si los parches recientemente instalados lo requieren. Ahora que se han completado todo el proceso de borrado y de parches, se puede habilitar la red y se puede informar al usuario final de que es posible el funcionamiento normal.

Actualizaciones menores de la aplicación

No todo el mantenimiento requiere las medidas drásticas descritas anteriormente. Si hay un parche disponible, pero no hay ningún ataque de virus en curso, es posible que sea adecuado aplicar un procedimiento menos drástico.

Un único script puede controlar el funcionamiento mediante la utilización de RETRYONERROR y de archivos de etiqueta.

1. **Fase de descarga**

   El proceso empieza con un recuadro de mensaje que informa al usuario final de que se descargará un parche para su posterior instalación. A continuación, el parche se puede copiar desde el servidor.

2. **Fase de parche**

   Ahora que el código de parche está listo para la instalación, es hora de avisar al usuario final e iniciar la instalación. Si el usuario final solicita un retraso, el archivo de etiqueta se puede utilizar para hacer un seguimiento del retraso. Quizás sean más urgentes solicitudes posteriores para instalar el parche. Tenga en cuenta que Antidote Delivery Manager mantiene este estado incluso si el usuario final apaga o rearranca su sistema. Cuando el usuario final ha otorgado el permiso, se instala el parche y se rearranca el sistema, si es necesario.

Cómo acomodar la seguridad de VPN y de redes inalámbricas

El entorno de Rescue and Recovery no da soporte actualmente a conexiones de VPN (Virtual Private Networks) de acceso remoto ni de redes inalámbricas. Si la máquina está utilizando una de estas conexiones de red en Windows XP y, a continuación, rearranca en Rescue and Recovery, se perderá la conectividad de red. Por lo tanto, un script como el del ejemplo anterior no funciona porque las comunicaciones de red no están disponibles en Rescue and Recovery para descargar archivos y arreglos.

Como solución puede empaquetar todos los archivos necesarios en el mensaje original o descargar los archivos necesarios antes de rearrancar. Esto se realiza colocando todos los archivos necesarios en el directorio con GO.RRS. El archivo de script se debe ocupar de mover los archivos necesarios a sus posiciones finales antes de salir del script (cuando se suprime el directorio que contiene GO.RRS). Es posible que la colocación de parches en el archivo del mensaje no sea práctica si los parches son muy grandes. En este caso, se debe informar al usuario final y, a continuación, restringir las comunicaciones de red sólo al servidor que contiene el parche. A continuación, el parche se puede descargar mientras se está todavía en

Windows XP. Aunque esto puede extender la exposición de Windows XP a un virus, este tiempo adicional probablemente no tiene ninguna importancia.

Capítulo 8. Prácticas recomendadas

Este capítulo presenta escenarios de uso para mostrar ejemplos de las prácticas recomendadas de Rescue and Recovery, Client Security Solution y del Software de huellas dactilares de ThinkVantage. Este escenario se inicia con la configuración de la unidad de disco duro, continúa con varias actualizaciones y sigue el ciclo vital de un despliegue. Se describe la instalación tanto en sistemas IBM como en sistemas no IBM.

Ejemplos de despliegue para instalar Rescue and Recovery y Client Security Solution

A continuación se presentan algunos ejemplos de la instalación de Rescue and Recovery y Client Security Solution en una máquina ThinkCentre y en un ThinkPad.

Ejemplo de despliegue de ThinkCentre

A continuación se muestra un ejemplo de una instalación en un ThinkCentre. Los requisitos hipotéticos del cliente que se utilizan son:

- **Administración**
  - Crear una copia de seguridad base de Sysprep con Rescue and Recovery.
  - Utilizar la cuenta de Administrador local para la administración del sistema.
- **Rescue and Recovery**
  - Utilizar la frase de paso de Client Security para proteger el acceso al espacio de trabajo de Rescue and Recovery.
    - El usuario debe iniciar sesión con su frase de paso y podrá abrir su archivo de volumen SafeGuard PrivateDisk para rescatar archivos.
- **Client Security Solution**
  - Instalarlo y ejecutarlo en modalidad de emulación.
    - No todos los sistemas IBM tienen un Módulo de plataforma segura (chip de seguridad).
  - Sin Password Manager
    - El cliente está utilizando en su lugar una solución de firma única de la empresa.
  - Habilitar la frase de paso de Client Security.
    - Proteger las aplicaciones de Client Security Solution mediante una frase de paso.
  - Habilitar el inicio de sesión de Windows de Client Security.
    - Iniciar sesión en Windows con la frase de paso de Client Security.
  - Crear SafeGuard PrivateDisk para todos los usuarios con un tamaño de 500 MB.
    - Cada usuario necesita 500 MB de espacio para almacenar datos de forma segura.
  - Habilitar la función de Recuperación de frase de paso de usuario final.
    - Permitir a los usuarios recuperar sus frases de paso respondiendo a tres preguntas y respuestas definidas por el usuario.

– Cifrar el script XML de Client Security Solution con contraseña = "ContScriptXML".
  - Proteger mediante contraseña el archivo de configuración de Client Security Solution.

En la máquina de preparación:

1. Inicie sesión con la cuenta del "Administrador local" de Windows.
2. Instale el programa Rescue and Recovery y Client Security Solution con las opciones siguientes:

   ```
   setup_tvtrnr3_1027.exe /s /v"/qn "EMULATIONMODE=1" "NOPWMANAGER=1"
   "NOCSSWIZARD=1""
   ```

   Notas:

   a. Asegúrese de que los archivos tvt, como por ejemplo z062zaa1025us00.tvt, están ubicados en el mismo directorio que el archivo ejecutable; de lo contrario, la instalación fallará.

   b. Si el archivo se denomina setup_tvtrnr3_1027c.exe, ha descargado el paquete combinado. Estas instrucciones son para los archivos que se han descargado de forma separada de la página de descarga ″Large Enterprise individual language files″.

   c. Si está realizando una instalación de Administrador, consulte "Instalación de Rescue and Recovery en un nuevo despliegue en sistemas Lenovo e IBM" en la página 127.

3. Después de rearrancar, inicie sesión con la cuenta del administrador local de Windows y prepare el script XML para el despliegue. Ejecute el siguiente mandato en la línea de mandatos:

   ```
   "C:\Archivos de programa\IBM ThinkVantage\Client Security Solution\
   css_wizarde.exe" /name:C:\ThinkCentre
   ```

   Seleccione las opciones siguientes en el Asistente:

   - Seleccione **Avanzadas -> Siguiente**.
   - Seleccione **Frase de paso de Client Security -> Siguiente**.
   - Seleccione **Iniciar sesión con la pantalla de inicio de sesión de Client Security -> Siguiente**.
   - Escriba la contraseña de Windows para la cuenta de administrador **-> Siguiente**.

     (WPW4Admin, por ejemplo)
   - Especifique la frase de paso de Client Security para la cuenta de administrador, seleccione el recuadro **Utilizar la frase de paso de Client Security para proteger el acceso al espacio de trabajo de Rescue and Recovery -> Siguiente**.

     (CSPP4Admin, por ejemplo)
   - Seleccione el recuadro **Habilitar recuperación de frase de paso** y seleccione tres preguntas y respuestas para la cuenta de administrador **-> Siguiente**

     a. ¿Cuál era el nombre de su primera mascota?

        (Fluffy, por ejemplo)

     b. ¿Cuál es su película favorita?

        (Lo que el viento se llevó, por ejemplo)

     c. ¿Cuál es su equipo de futbol favorito?

        (F.C. Barcelona, por ejemplo)

- No seleccione **Crear un volumen PrivateDisk para cada usuario, con el tamaño seleccionado a continuación**. **-> Siguiente**.
- Revise el Resumen y seleccione **Aplicar** para grabar el archivo xml en la siguiente ubicación C:\ThinkCentre.xml **-> Aplicar**.
- Seleccione **Finalizar** para cerrar el asistente.

4. Abra el archivo siguiente en un editor de texto (los editores de scripts XML o Microsoft Word 2003 tiene funciones de formato XML incorporadas) y modifique los siguientes valores:
   - Elimine todas las referencias al valor Domain. Esto indicará al script que utilice en su lugar el nombre de la máquina local en cada sistema. Guarde el archivo.
5. Utilice la herramienta que se encuentra en C:\Archivos de programa\IBM ThinkVantage\Client Security Solution\xml_crypt_tool.exe para cifrar el script XML con una contraseña. Ejecute el archivo desde un indicador de mandatos, utilizando la sintaxis siguiente:
   a. xml_crypt_tool.exe C:\ThinkCentre.xml /encrypt XMLScriptPW
   b. Este archivo se llamará ahora C:\ThinkCentre.xml.enc y estará protegido mediante la contraseña = XMLScriptPW

El archivo C:\ThinkCentre.xml.enc está ahora preparado para ser añadido a la máquina de despliegue.

En la máquina de despliegue:

1. Inicie sesión con la cuenta del administrador local de Windows.
2. Instale los programas Rescue and Recovery y Client Security Solution con las opciones siguientes:

   ```
   setup_tvtrnr3_1027.exe /s /v"/qn "EMULATIONMODE=1" "NOPWMANAGER=1"
   "NOCSSWIZARD=1""
   ```

   Notas:

   a. Asegúrese de que el archivo o los archivos tvt, como por ejemplo z062zaa1025us00.tvt, están ubicados en el mismo directorio que el archivo ejecutable; de lo contrario, la instalación fallará.
   b. Si el archivo se denomina setup_tvtrnr3_1027c.exe, ha descargado el paquete combinado. Estas instrucciones son para los archivos que se han descargado de forma separada de la página de descarga ″Large Enterprise individual language files″.
   c. Si está realizando una instalación de Administrador, consulte “Instalación de Rescue and Recovery en un nuevo despliegue en sistemas Lenovo e IBM” en la página 127.
3. Después de rearrancar, inicie sesión con la cuenta del administrador local de Windows.
4. Añada el archivo ThinkCentre.xml.enc preparado anteriormente al directorio raíz C:\.
5. Modifique el registro para establecer el Tamaño por omisión del volumen SafeGuard PrivateDisk = 500 MB para todos los usuarios. Esto se consigue fácilmente mediante la importación de un archivo *reg*.
   a. Vaya a: HKEY_LOCAL_MACHINE\SOFTWARE\IBM ThinkVantage\Client Security Software.
   b. Cree un nuevo Valor de serie de caracteres con el nombre de Valor: = PrivateDiskSize y un dato de Valor: = 500.

c. Cree un Valor DWORD con el nombre de Valor: = UsingPrivateDisk y un dato de Valor: = 1.

6. Prepare el mandato RunOnceEx con los parámetros siguientes.
   - Añada una nueva clave a la clave RunonceEx denominada “0001”. Debe ser: HKEY_LOCAL_MACHINE \Software\Microsoft\Windows\Current Version\RunOnceEx\0001
   - En dicha clave añada un nombre de valor de serie de caracteres “CSSEnroll” con el valor: ″c:\Archivos de programa\IBM ThinkVantage\Client Security Solution\vmservere.exe” C:\ThinkCenter.xml.enc XMLscriptPW
7. Ejecute “%rr%\rrcmd.exe sysprepbackup location=L name=”Sysprep Backup”. Después de que haya preparado el sistema, verá esta salida:

```
*****************************************************
** Ready to take sysprep backup.                    **
**                                                  **
** PLEASE RUN SYSPREP NOW AND SHUT DOWN.            **
**                                                  **
** Next time the machine boots, it will boot        **
** to the PreDesktop Area and take a backup.        **
*****************************************************
```

8. Ejecute ahora la implementación de Sysprep.
9. Concluya y rearranque la máquina. Iniciará el proceso de copia de seguridad en Windows PE.

   Nota: NOTA: Indicará que la restauración está en curso aunque se esté realizando una copia de seguridad. Después de la copia de seguridad, APAGUE EL SISTEMA y no reinicie.

Ahora la copia de seguridad base de Sysprep se ha completado

Ejemplo de despliegue en un Thinkpad

A continuación se muestra ejemplo de una instalación en un ThinkPad: Los requisitos hipotéticos del cliente que se utilizan son:

- **Administración**
  - Instalar en sistemas de los que ya se ha creado una imagen y que ya se han desplegado.
  - Utilizar la cuenta del administrador de dominio para la administración del sistema.
  - Todos los sistemas tienen una cuenta de supervisor del BIOS, BIOSpw.
- **Client Security Solution**
  - Aprovechar el Módulo de plataforma fiable
    - Todas las máquinas tienen el chip de seguridad.
  - Habilitar Password Manager
  - Inhabilitar SafeGuard PrivateDisk
    - Utilizar, en su lugar, el cifrado de toda la unidad de disco duro de Utimaco SafeGuard Easy
  - Utilizar la contraseña de Windows del usuario como autentificación en Client Security Solution.
    - Permitir la autentificación mediante una única contraseña de Windows en Utimaco SafeGuard Easy, Client Security Solution y el dominio de Windows.
  - Cifrar el script XML de Client Security Solution XML con contraseña = ″XMLscriptPW″.

- La contraseña protege el archivo de configuración de Client Security Solution

- Software de huellas dactilares de **ThinkVantage**
  - No desea aprovechar las contraseñas del BIOS y del disco duro.
  - Iniciar sesión mediante huella dactilar
    - Después de un período inicial de autoregistro del usuario, el usuario conmutará al inicio de sesión en Modalidad segura que requiere una huella dactilar para los usuarios no administradores, imponiendo, por lo tanto, de forma efectiva una metodología de autentificación de dos factores.
  - Incluir la Guía de aprendizaje de huellas dactilares
    - Los usuarios finales pueden aprender cómo pasar correctamente el dedo y obtener una respuesta visual acerca de lo que hacen incorrectamente.

En la máquina de preparación:

1. Desde el estado de apagado, inicie el sistema y pulse **F1** para ir al BIOS y navegar hasta el menú de seguridad y borrar el chip de seguridad. Guarde y salga del BIOS.
2. Inicie sesión con la cuenta de administrador de dominio de Windows.
3. Instale el Software de huellas dactilares de ThinkVantage ejecutando el archivo f001zpz2001us00.exe para extraer el archivo setup.exe del paquete Web. Esto extraerá automáticamente el archivo setup.exe en la siguiente ubicación: C:\IBMTOOLS\APPS\TFS4.6-Build1153\Application\0409\setup.exe.
4. Instale la Guía de aprendizaje de huellas dactilares de ThinkVantage ejecutando el archivo f001zpz7001us00.exe para extraer el archivo tutess.exe del paquete Web. Esto extraerá automáticamente el archivo setup.exe en la siguiente ubicación: C:\IBMTOOLS\APPS\tutorial\TFS4.6-Build1153\Tutorial\0409\tutess.exe.
5. Instale la Consola de huellas dactilares de ThinkVantage ejecutando el archivo f001zpz5001us00.exe para extraer el archivo fprconsole.exe del paquete Web. La ejecución del archivo f001zpz5001us00.exe extraerá automáticamente el archivo setup.exe en la siguiente ubicación: C:\IBMTOOLS\APPS\fpr_con\APPS\UPEK\FPR Console\TFS4.6-Build1153\Fprconsole\fprconsole.exe.
6. Instale el programa Client Security Solution con las opciones siguientes:

   ```
   setup_tvtcss6_1027.exe /s /v"/qn NOPRVDISK=1 NOCSSWIZARD=1 SUPERVISORPW=
   "BIOSpw""
   ```

7. Después de rearrancar, inicie sesión con la cuenta del administrador de dominio de Windows y prepare el script XML para el despliegue. En la línea de mandatos ejecute:

   ```
   "C:\Archivos de programa\IBM ThinkVantage\Client Security Solution\
   css_wizard.exe" /name:C:\ThinkPad
   ```

   Seleccione las opciones siguientes en el Asistente para que coincidan con el script de ejemplo:

   - Seleccione Avanzadas **-> Siguiente**.
   - Seleccione la contraseña de Windows **-> Siguiente**.
   - Seleccione Iniciar sesión con el sensor de huellas dactilares **-> Siguiente**.
   - Escriba la contraseña de Windows para la cuenta del administrador de dominio **-> Siguiente**.

     (WPW4Admin, por ejemplo)
   - • Deseleccione Habilitar recuperación de contraseña **-> Siguiente**.

- • Revise el Resumen y seleccione Aplicar para grabar el archivo xml en la siguiente ubicación C:\ThinkPad.xml.
- • Seleccione **Finalizar** para cerrar el asistente.

8. Utilice la herramienta que se encuentra en C:\Archivos de programa\IBM ThinkVantage\Client Security Solution\xml_crypt_tool.exe para cifrar el script XML con una contraseña. En un indicador de mandatos, utilice la siguiente sintaxis:
   a. xml_crypt_tool.exe C:\ThinkPad.xml /encrypt XMLScriptPW
   b. El archivo se llamará ahora C:\ThinkPad.xml.enc y estará protegido por la contraseña = XMLScriptPW.

En la máquina de despliegue:

1. Utilizando las herramientas de distribución de software de la empresa, despliegue en cada máquina de despliegue el ejecutable setup.exe del Software de huellas dactilares de ThinkVantage que se ha extraído de la máquina de preparación. Cuando el archivo setup.exe llegue a la máquina, instálelo mediante el mandato siguiente:

   ```
   setup.exe CTLCNTR=0 /q /i
   ```

2. Utilizando las herramientas de distribución de software de la empresa, despliegue en cada máquina de despliegue el ejecutable tutess.exe de la Guía de aprendizaje de huellas dactilares de ThinkVantage que se ha extraído de la máquina de preparación. Cuando el archivo tutess.exe llegue a la máquina, instálelo mediante el mandato siguiente:

   ```
   tutess.exe /q /i
   ```

3. Utilizando las herramientas de distribución de software de la empresa, despliegue en cada máquina de despliegue el ejecutable fprconsole.exe de la Consola de huellas dactilares de ThinkVantage que se ha extraído de la máquina de preparación.
   - Coloque el archivo fprconsole.exe en el directorio “C:\Archivos de programa\ThinkVantage Fingerprint Software\”
   - Desactive el soporte de seguridad de encendido del BIOS ejecutando el mandato siguiente: fprconsole.exe settings TBX 0
4. Utilizando las herramientas de distribución de software de la empresa, despliegue el ejecutable “setup_tvtcss6_1027.exe”de ThinkVantage Client Solution.
   - Cuando el archivo setup_tvtcss6_1027.exe llegue a la máquina, instálelo mediante el mandato siguiente: setup_tvtcss6_1027.exe /s /v”/qn NOPRVDISK=1 NOCSSWIZARD=1 SUPERVISORPW=”BIOSpw””
   - La instalación del software habilitará automáticamente el hardware del Módulo de plataforma fiable.
5. Después de rearrancar el sistema, configure el sistema mediante el archivo script XML mediante el procedimiento siguiente:
   - Copie el archivo ThinkPad.xml.enc preparado anteriormente en el directorio C:\.
   - Ejecute C:\Archivos de programa\IBM ThinkVantage\Client Security Solution\vmserver.exe C:\ThinkPad.xml.enc XMLScriptPW
6. Después de rearrancar, el sistema estará ahora preparado para el registro de usuario de Client Security Solution. Cada usuario puede iniciar sesión en el sistema con su ID de usuario y su contraseña de Windows. A cada usuario que inicie sesión en el sistema se le solicitará automáticamente que se registre en Client Security Solution y, a continuación, se podrá registrar en el lector de huellas dactilares.

7. Después de que todos los usuarios del sistema se hayan registrado en el Software de huellas dactilares de ThinkVantage, se puede habilitar el valor de Modalidad segura para hacer que todos los usuarios no administradores de Windows tengan que iniciar sesión con la huella dactilar.
   - Ejecute el mandato siguiente: C:\Archivos de programa\ThinkVantage Fingerprint Software\fprconsole.exe settings securemode 1
   - Para eliminar el mensaje Pulse CTRL+ALT+DEL para iniciar sesión utilizando una contraseña, en la pantalla de inicio de sesión, ejecute el mandato siguiente:

     ```
     C:\Archivos de programa\ThinkVantage Fingerprint Software\fprconsole.exe
     settings CAD 0
     ```

Ahora se ha completado el despliegue de Client Security Solution 6.0 y del Software de huellas dactilares de ThinkVantage.

Instalación de Rescue and Recovery en un nuevo despliegue en sistemas Lenovo e IBM

Esta sección describe la instalación de Rescue and Recovery en un nuevo despliegue.

Preparación de la unidad de disco duro

El primer paso que se debe tener en cuenta al desplegar un sistema es la preparación de la unidad de disco duro en el sistema donante. Para tener la completa seguridad de que va a empezar con un disco duro limpio, debe borrar el Registro de arranque maestro del disco duro primario.

1. Extraiga todos los dispositivos de almacenamiento, como por ejemplo segundos discos duros, discos duros USB, llaves de memoria USB, memoria de Tarjeta PC, etc, del sistema donante, excepto el disco duro primario en el que va a instalar Windows.

   Atención: La ejecución de este mandato borrará todo el contenido de la unidad de disco duro de destino. Después de ejecutarlo, no podrá recuperar ningún dato de la unidad de disco duro de destino.
2. Cree un disquete de arranque de DOS y coloque el archivo CLEANDRV.EXE en él.
3. Arranque el disquete (sólo con un dispositivo de almacenamiento conectado). En el indicador de DOS, escriba el mandato siguiente:

   ```
   CLEANDRV /HDD=0
   ```
4. Instale el sistema operativo y las aplicaciones. Cree el sistema donante como si no estuviera instalando Rescue and Recovery. El último paso del proceso es instalar Rescue and Recovery.

Instalación

El primer paso del proceso de instalación es la extracción del ejecutable de InstallShield del directorio C:\RRTEMP. Si va a instalar Rescue and Recovery en varios sistemas, la realización de este proceso una vez reducirá el tiempo de instalación en cada máquina a aproximadamente la mitad.

1. Presuponiendo que el archivo de instalación esté ubicado en la raíz de la unidad C, cree un archivo EXE_EXTRACT.CMD, que extraerá el archivo C:\SETUP_TVTRNR3_*XXXX*.EXE (donde *XXXX* es el ID de build) al directorio C:\RRTEMP:

   ```
   :: Este paquete extraerá el archivo WWW EXE en el directorio c:\RRTemp para una
   :: instalación administrativa.
   ```

```
@ECHO OFF
:: Es el nombre del EXE (sin la terminación .EXE)
set BUILDID=setup_tvtrnr3_1027.exe
:: Es la letra de la unidad del archivo Setu_tvtrnr3_1027.exe
:: NOTA: NO FINALICE LA CADENA DE CARACTERES CON "\".  SE ASUME QUE NO ESTÁ.
SET SOURCEDRIVE=C:
:: Cree el directorio RRTemp en la unidad de disco duro para el archivo WWW EXMD
:: que se ha extraído c:\RRTemp
:: Extrae el archivo WWW EXE en el directorio c:\RRTemp
:: Nota: Se debe copiar el archivo TVT.TXT en el mismo directorio que el
:: archivo MSI.EXE.
start /WAIT %SOURCEDRIVE%\%BUILDID%.exe /a /s /v"/qn TARGETDIR=c:\RRTemp"
 TARGETDIR=c:\RRTemp"
Copie Z062ZAA1025US00.TVT C:\rrtemp\
```

2. Puede realizar muchas personalizaciones antes de la instalación de Rescue and Recovery. Algunos ejemplos de este escenario son:
   - Cambie el número máximo de copias de seguridad incrementales a 4.
   - Establezca Rescue and Recovery para que realice una copia de seguridad incremental cada día a la 1:59 p.m. de la unidad de disco duro local y llámela Planificada.
   - Oculte la interfaz de usuario de Rescue and Recovery a todos los usuarios que no están en el grupo de administradores locales.
3. Cree un archivo TVT.TXT de personalización. Se pueden modificar algunos parámetros. Consulte Apéndice B, “Parámetros y valores de TVT.TXT”, en la página 149 para obtener más información.

```
[Scheduler]
Task1=RescueRecovery
Task2=egatherer
Task3=logmon

[egatherer]
ScheduleMode=0x04
Task=%TVT%\Rescue and Recovery\launcheg.exe
ScheduleHour=0
ScheduleMinute=0
ScheduleDayOfTheWeek=0
ScheduleWakeForBackup=0


[RescueRecovery]
LastBackupLocation=1
CustomPartitions=0
Exclude=0
Include=0
MaxNumberOfIncrementalBackups=5
EncryptUsingCSS=0
HideCSSEncrypt=0
UUIDMatchRequired=0
PasswordRequired=0
DisableSchedule=0
DisableRestore=0
DisableSFR=0
DisableViewBackups=0
DisableArchive=0
DisableExclude=0
DisableSingleStorage=0
DisableMigrate=0
DisableDelete=0
DisableAnalyze=0
DisableSysprep=1
```

```
CPUPriority=3
Yield=0
Ver=4.1
DisableBackupLocation=0
DeletedBackupLocation=0
HideLocationNotFoundMsg=0
HideMissedBackupMessage=0
HideNoBatteryMessage=0
SkipLockedFiles=0
DisableBootDisc=0
DisableVerifyDisc=0
HideAdminBackups=0
HideBaseFromDelete=0
HidePasswordProtect=0
HideSuspendCheck=1
HideBootUSBDialog=0
HideBootSecondDialog=1
HideNumBackupsDialog=1
HidePasswordPersistence=0
HideDiffFilesystems=0
PwPersistence=0
ParseEnvironmentVariables=1
MinAnalyzeFileSize=20
HideLockHardDisk=1
LockHardDisk=0
ResumePowerLossBackup=1
MinPercentFreeSpace=0
MaxBackupSizeEnforced=0
PreRejuvenate=
PreRejuvenateParameters=
PreRejuvenateShow=
PostRejuvenate=
PostRejuvenateParameters=
PostRejuvenateShow=
RunSMA=1
SPBackupLocation=0
ScheduleMode=4
ScheduleFrequency=2
ScheduleHour=12
ScheduleMinute=0
ScheduleDayOfTheMonth=0
ScheduleDayOfTheWeek=3
ScheduleWakeForBackup=0
Task=%TVT%\Rescue and Recovery\rrcmd.exe
TaskParameters=BACKUP location=L name="Scheduled" scheduled
SetPPArchiveBeforeBackup=1

[RestoreFilesFolders]
WinHiddenFolders=%RRBACKUPS%,%MININT%,%PREBOOT%,%HIBERFIL%,%PAGEFILE%,
%SYSVOLINFO%,%RECYCLER%
PEHiddenFolders=%RRBACKUPS%,%MININT%,%PREBOOT%,%HIBERFIL%,%PAGEFILE%,
%SYSVOLINFO%,%RECYCLER%,Z:\
AllowDeleteC=FALSE

[logmon]
ScheduleMode=0x010
Task=%TVT%\Common\Logger\logmon.exe
```

4. En el mismo directorio que el archivo TVT.TXT personalizado, cree un archivo INSTALL.CMD, que realizará varias acciones:
   - Copie el archivo TVT.TXT personalizado en el paquete de instalación creado en el directorio C:\RRTemp:
   - Realice una instalación silenciosa de Rescue and Recovery sin un rearranque al final.
   - Inicie Rescue and Recovery de forma que se puede realizar una copia de seguridad base.

- Después de que se inicie el servicio, configure el entorno para crear una imagen ISO del CD de Rescue and Recovery (esto se realiza normalmente como parte de un rearranque).
- Cree una imagen ISO.
- Cree la copia de seguridad base y rearranque el sistema.

5. Modifique el código de INSTALL.CMD. Lo siguiente representa el código de INSTALL.CMD:

```
:: Copie aquí el archivo TVT.txt personalizado

copy tvt.txt "c:\RRTemp\Archivos de programa\IBM ThinkVantage\Rescue and Recovery"

:: Instálelo utilizando el MSI sin rearranque (Elimine "REBOOT="R"" para forzar un
:: rearranque)

start /WAIT msiexec /i "c:\TVTRR\Rescue and Recovery - client security
 solution.msi" /qn REBOOT="R"

:: Inicie el servicio. Esto es necesario para crear una copia de seguridad base.

start /WAIT net start "Servicio de Rescue and Recovery"

:: Cree aquí un archivo ISO - ISO residirá en c:\Archivos de programa\IBM
ThinkVantage\Rescue and Recoveery\rrcd
```

Nota: No necesita configurar el entorno si se ha rearrancado el sistema.

```
:: Configure el entorno

set PATH=%PATH%;%SystemDrive%\Archivos de programa\IBM ThinkVantage\Common\Python24

set PATHEXT=%PATHEXT%;.PYW;.PYO;.PYC;.PY

set TCL_LIBRARY=%SystemDrive%\Archivos de programa\IBM ThinkVantage\Common\Python24
\tcl\tcl8.4

set TK_LIBRARY=%SystemDrive%\Archivos de programa\IBM ThinkVantage\Common\Python24
\tcl\tk8.4

set PYTHONCASEOK=1

set RR=C:\Archivos de programa\IBM ThinkVantage\Rescue and Recovery\

set PYTHONPATH=C:\Archivos de programa\IBM ThinkVantage\Common\logger

:: La siguiente línea creará el archivo ISO de forma silenciosa y no lo grabará

C:\Archivos de programa\IBM ThinkVantage\Common\Python24\python C:\Archivos de
programa\IBM ThinkVantage\Common\spi\mkspiim.pyc /scripted

:: Realice la copia de seguridad base... se debe iniciar el servicio

c:

cd "C:\Archivos de programa\IBM ThinkVantage\Rescue and Recovery"

RRcmd.exe backup location=L name=Base level=0

:: Rearranque el sistema

C:\Archivos de programa\IBM ThinkVantage\Common\BMGR\bmgr32.exe /R
```

Personalización

Ha desplegado Rescue and Recovery en el entorno y desea cambiar los elementos siguientes con Rescue and Recovery :

- Desea más de 4 copias de seguridad incrementales y desea cambiarlo a 10.
- La hora de copia de seguridad de la 1:59 p.m. interfiere de alguna forma con el entorno. Desea cambiar la hora a las 10:24 a.m.
- Desea permitir que todos los usuarios accedan a la interfaz de usuario de Rescue and Recovery 3.0.
- Desea que el proceso de prioridad a otros procesos durante una copia de seguridad planificada. La evaluación después de la experimentación determina que el valor correcto de `Yield=` en el entorno debe ser `2` en lugar del valor estándar de `0`.

Para realizar estos cambios en varias máquinas:

1. Cree un archivo mod denominado UPDATE.MOD (utilizando un editor de texto) con el contenido siguiente:

   ```
   [RescueRecovery] MaxNumberOfIncrementalBackups=10
   [rescuerecovery] ScheduleHour=10
   [rescuerecovery] ScheduleMinute=24
   [rescuerecovery] GUIGroup=
   [rescuerecovery] Yield=2
   ```

2. A continuación, puede crear un archivo INSTALL.CMD y utilizar la herramienta de gestión del sistema de su elección para enviar los archivos INSTALL.CMD y UPDATE.MOD a los sistemas de destino. Después de que los sistemas hayan ejecutado el archivo INSTALL.CMD, las actualizaciones serán efectivas. El contenido del archivo INSTALL.CMD es el siguiente:

   ```
   :: Fusione los cambios en TVT.TXT
   "%RR%cfgmod.exe" "%RR%tvt.txt" update.mod
   :: Restablezca el planificador para que adopte la nueva copia de copia de
   seguridad planificada sin un rearranque
   "%RR%reloadsched.exe"
   ```

Actualización

Es posible que necesite realizar un cambio importante en el sistema, como por ejemplo una actualización de un paquete de servicio de Windows. Antes de instalar el Service Pack, haga una copia de seguridad incremental en el sistema e identifique dicha copia de seguridad por nombre realizando los pasos siguientes:

1. Cree un archivo FORCE_BU.CMD y envíelo a los sistemas de destino.
2. Inicie el archivo FORCE_BU.CMD una vez que esté en el sistema de destino.

El contenido del archivo FORCE_BU.CMD es:

```
:: Fuerce una copia de seguridad ahora
"%RR%rrcmd" backup location=L name="Copia de seguridad antes de actualización XP-SP2"
```

Habilitación del escritorio de Rescue and Recovery

Después de darse cuenta de las ventajas de Rescue and Recovery durante un período de tiempo, es posible que desee beneficiarse del entorno de Rescue and Recovery. A fines de demostración, en la siguiente sección se proporciona un script UPDATE_RRE.CMD de ejemplo que extraerá el archivo de control para el entorno de Rescue and Recovery, que puede editar y, a continuación, poner de nuevo en el entorno de Rescue and Recovery utilizando RRUTIL.exe. Consulte “Utilización de RRUTIL.EXE” en la página 22 para obtener más información.

Para modificar el Área previa al escritorio, el script UPDATE_RRE.CMD script hace una demostración de varios procesos:

- Utilice RRUTIL.exe para obtener un archivo del entorno de Rescue and Recovery. Los archivos que se estraerán del entorno de Rescue and Recovery están definidos en el archivo GETLIST.TXT.
- Cree una estructura de directorios para poner de nuevo los archivos en el Área previa al escritorio después de editar el archivo adecuado.
- Realice una copia del archivo por razones de seguridad y, a continuación, edítelo.

En este ejemplo, desea cambiar la página inicial que se abre cuando un usuario final pulsa el botón **Abrir navegador** en el entorno de Rescue and Recovery. Se abrirá la página Web `http://www.lenovo.com/thinkvantage`.

Para realizar el cambio, cuando se abra el Bloc de notas con el archivo PEACCESSIBMEN.INI haga lo siguiente:

1. Cambie la línea:

   ```
   button13 = 8, "Abrir navegador", Internet.bmp, 1, 1, 0,
   %sysdrive%\Preboot\Opera\Opera.EXE, http://www.pc.ibm.com/cgi-
   bin/access_IBM.cgi?version=4&link=gen_support&country=__
   COUNTRY__&language=__LANGUAGE__
   ```

   A

   ```
   button13 = 8, "Abrir navegador", Internet.bmp, 1, 1, 0,
   %sysdrive%\Preboot\Opera\Opera.EXE,
    http://www.ibm.com/thinkvantage
   ```

2. Ponga la nueva versión en la estructura de directorios para colocar los archivos en el entorno de Rescue and Recovery. Para ver más detalles, consulte "Utilización de RRUTIL.EXE" en la página 22.
3. Rearranque el sistema en el entorno de Rescue and Recovery.
4. Ha realizado algunos análisis y ha determinado que existen archivos de los que debe realizar una copia de seguridad y otros archivos de los que no necesita realizar una copia de seguridad porque están ubicados en el servidor y se pueden obtener después de una restauración del sistema. Para hacer esto, cree un archivo IBMFILTER.TXT personalizado. Este archivo se coloca en un directorio con el archivo NSF.CMD, que lo copia en la ubicación correcta tal y como se muestra en el ejemplo siguiente:

   NSF.CMD:

   ```
   copy ibmfilter.txt "%RR%"
   ```

   IBMFILTER.TXT:

   ```
   x=*.nsf
   ```

Tabla 37. Script UPDATE_RR.CMD

```
@ECHO OFF
::Obtenga el archivo PEAccessIBMen.ini de RR
c:\RRDeployGuide\RRUTIL\RRUTIL -g getlist.txt
c:\RRDeployGuide\GuideExample\RROriginal
:: Cree un directorio donde poner el archivo editado para importar de nuevo en RR
md c:\RRDeployGuide\GuideExample\put\preboot\usrintfc
:: Abra el archivo con el Bloc de notas y edítelo.
ECHO.
ECHO Edite el archivo
c:\RRDeployGuide\GuideExample\RROriginal\PEAccessIBMen.ini

El archivo se abrirá automáticamente

pause
:: Realice una copia del archivo original
copy
c:\RRDeployGuide\GuideExample\RROriginal\preboot\usrintfc\PEAccessIBMen.ini
c:\RRDeployGuide\GuideExample\RROriginal\preboot\usrintfc\
PEAccessIBMen.original.ini
notepad
c:\RRDeployGuide\GuideExample\RROriginal\preboot\usrintfc\PEAccessIBMen.ini
pause
copy c:\RRDeployGuide\GuideExample\RROriginal\preboot\usrintfc\
PEAccessIBMen.ini c:\RRDeployGuide\GuideExample\put\preboot\usrintfc
:: Coloque la versión actualizada de PEAccessIBMen en RR
c:\RRDeployGuide\RRUTIL\RRUTIL -p c:\RRDeployGuide\GuideExample\put
ECHO.
ECHO Rearranque RR para ver el cambio
pause
c:\Archivos de programa\IBM ThinkVantage\Common\BMGR\bmgr32.exe /bw /r

Cree GETLIST.TXT:

\preboot\usrintfc\PEAccessIBMen.ini
```

Instalación de Rescue and Recovery en sistemas no IBM

Para instalar Rescue and Recovery, debe haber disponibles ocho sectores en el Registro de arranque maestro del disco duro. Rescue and Recovery utiliza un Registro de arranque maestro para entrar en el área de Recuperación.

Algunos OEM almacenan punteros a su código de recuperación del producto en el sector del Registro de arranque maestro. El código de recuperación del producto del OEM puede interferir con la instalación del Gestor de arranque maestro de Rescue and Recovery.

Tenga en cuenta los escenarios siguientes y las prácticas recomendadas para ayudarle a garantizar que Rescue and Recovery proporciona las funciones y las características deseadas:

Prácticas recomendadas para la configuración del disco duro: Escenario 1

Este escenario trata el nuevo despliegue de una imagen que incluye Rescue and Recovery. Si se despliega Rescue and Recovery en clientes OEM existentes que contengan el código de recuperación del producto OEM, ejecute la prueba siguiente para determinar si el código de recuperación del producto OEM interfiere con Rescue and Recovery:

1. Configure un cliente de prueba con la imagen que contiene el código de recuperación del producto OEM.

2. Instale Rescue and Recovery. Si no existen ocho sectores libres en el MBR como resultado del código de recuperación del producto OEM, verá el siguiente mensaje de error:

   ```
   Error 1722. Existe un problema con este paquete de
   Windows Installer. Un programa ejecutado como parte de
   la instalación no ha finalizado de la forma esperada. Póngase en contacto con
   el personal o el proveedor del paquete.
   ```

Si está utilizando una imagen del OEM para el sistema operativo base, asegúrese de que el Registro de arranque maestro no contiene los datos de recuperación del producto. Puede hacer esto de la forma siguiente:

Atención: La ejecución del siguiente mandato borrará todo el contenido de la unidad de disco duro de destino. Después de ejecutarlo, no podrá recuperar ningún dato de la unidad de disco duro de destino.

1. Utilice el archivo CLEANDRV.EXE disponible en la sección de las herramientas administrativas en:

   ```
   http://www.lenovo.com/ThinkVantage
   ```

   para asegurarse de que se han borrado todos los sectores del Registro de arranque maestro de la unidad de disco duro que planea utilizar para crear la imagen base.
2. Empaquete la imagen según los procedimientos para el despliegue.

Prácticas recomendadas para la configuración del disco duro: Escenario 2

El despliegue del programa Rescue and Recovery en clientes existentes requiere cierto esfuerzo y planificación.

Si recibe el Error 1722 y necesita crear ocho sectores libres, llame a IBM Help Desk para informar del error y obtener más instrucciones.

Creación de un CD arrancable de Rescue and Recovery

Rescue and Recovery crea y graba el CD del soporte de rescate a partir del contenido actual del área de servicio, en lugar de hacerlo a partir de la imagen ISO montada previamente. Sin embargo, si ya está presente una imagen ISO adecuada, porque estaba precargada o porque se ha creado anteriormente, esta imagen se utilizará para grabar el CD, en lugar de la nueva imagen.

Debido a los recursos implicados, sólo se puede ejecutar simultáneamente una instancia de una aplicación de grabación de CD. Si se grabando y se intenta iniciar una segunda instancia se producirá un mensaje de error y se abortará la segunda instancia. Además, debido a la naturaleza de acceder a áreas protegidas del disco duro, sólo los administradores pueden crear la ISO; sin embargo, un usuario final con limitaciones puede grabar la ISO en un CD. Estos archivos y directorios se incluirán en el CD de recuperación:

- minint
- preboot
- win51
- win51ip
- win51ip.sp1
- scrrec.ver

Nota: Si crea una nueva imagen ISO, debe tener como mínimo 400 MB de espacio libre disponible en la unidad del sistema a fin de copiar los árboles de directorios y crear la ISO. Mover tantos datos implica mucho trabajo en el disco duro, y es posible que se tarde 15 minutos o más en algunos sistemas.

Creación del archivo ISO de recuperación y grabación en un CD de un archivo script de ejemplo: Prepara el código siguiente:

```
:: Cree aquí un archivo ISO - ISO residirá en c:\IBMTOOLS\rrcd
```

Nota: Las siguientes siete líneas de código (en negrita) son necesarias sólo si no se rearranca el sistema después de la instalación.

```
:: Configure el entorno
set PATH=%PATH%;%SystemDrive%\Archivos de programa\IBM ThinkVantage\Common\Python24
set PATHEXT=%PATHEXT%;.PYW;.PYO;.PYC;.PY
set TCL_LIBRARY=%SystemDrive%\Archivos de programa\IBM ThinkVantage\Common\Python24
\tcl\tcl8.4
set TK_LIBRARY=%SystemDrive%\Archivos de programa\IBM ThinkVantage\Common\Python24
\tcl\tk8.4
set PYTHONCASEOK=1
set RR=c:\Archivos de programa\IBM ThinkVantage\Rescue and Recovery\
set PYTHONPATH=C:\Program files\IBM ThinkVantage\Common\logger
:: La siguiente línea creará el archivo ISO de forma silenciosa y no lo grabará
c:\Archivos de programa\IBM ThinkVantage\Common\Python24\python c:\Archivos de
programa\IBM ThinkVantage\Common\spi\mkspiim.pyc /scripted
:: La línea siguiente creará la ISO con la interacción del usuario y no la grabará
:: c:\Archivos de programa\IBM ThinkVantage\Common\Python24\python c:\Archivos de
programa\IBM ThinkVantage\Common\spi\mkspiim.pyc /scripted
/noburn
```

Instalación de Rescue and Recovery en una partición de servicio de tipo 12

Debe tener lo siguiente para poder instalar Rescue and Recovery en una partición de servicio de tipo 12:

- El archivo SP.PQI. Este archivo incluye archivos arrancables base para crear una partición de servicio.
- PowerQuest PQDeploy
- El instalador más reciente de Rescue and Recovery

Existen varias opciones relativas a la instalación de Rescue and Recovery en una partición de servicio.

Nota: La partición de tipo 12 debe residir en la última entrada utilizada de la tabla de particiones de la misma unidad que contiene Windows en la unidad C:\. Puede utilizar bmgr32 /info para determinar dónde reside la partición de tipo 12 en la unidad de disco duro. Para obtener más información, consulte “Control del Gestor de arranque de Rescue and Recovery (BMGR32)” en la página 171.

Para realizar la instalación, complete el procedimiento siguiente:

1. Deje como mínimo 700 MB de espacio libre sin asignar al final de la unidad.
2. Utilizando PowerQuest, restaure el archivo SP.PQI al espacio libre no asignado.
3. Suprima las particiones primarias creadas en el paso 1 (excepto la unidad C) y, a continuación, rearranque.

Nota: La información de volumen del sistema puede estar en la partición de servicio que se acaba de crear. Es necesario suprimir la información de volumen del sistema mediante la Restauración del sistema de Windows.

4. Instale Rescue and Recovery y rearranque cuando se le solicite.

Copia de seguridad/restauración de Sysprep

Tenga en cuenta que la Persistencia de contraseña no funcionará con Copia de seguridad/restauración de Sysprep.

Debe apagar y rearrancar el sistema después de completar la copia de seguridad de Sysprep.

Computrace y Rescue and Recovery

En sistema sin BIOS, Rescue and Recovery no se puede desinstalar una vez que se ha instalado Computrace.

Capítulo 9. Software de huellas dactilares

La consola de huellas dactilares se debe ejecutar desde la carpeta de instalación del Software de huellas dactilares. La sintaxis básica es FPRCONSOLE [USER | SETTINGS]. El mandato USER o SETTINGS especifica qué conjunto de la operación se utilizará. El mandato completo será, por ejemplo, "fprconsole user add TestUser /FORCED". Cuando no se conoce el mandato o no se especifican todos los parámetros, se mostrará una corta lista de mandatos junto con los parámetros.

Para descargar el Software de huellas dactilares y la Consola de gestión, utilice por favor el enlace siguiente

http://www.lenovo.com/think/support/site.wss/document.do?sitestyle=lenovo&indocid=TVAN-EAPFPR

Mandatos específicos del usuario

Para registrar o editar usuarios se utiliza la sección USER. Cuando el usuario actual no tiene derechos de administrador, el comportamiento de la consola depende de la modalidad de seguridad del sistema de archivos. Modalidad cómoda: para el usuario estándar son posibles los mandatos ADD, EDIT y DELETE. Sin embargo, el usuario puede modificar sólo su propio pasaporte (registrado con su usuario). Modalidad segura: no se permite ningún mandato. Sintaxis:

`FPRCONSOLE USER` *`mandato`*

donde *mandato* es uno de los mandatos siguientes: ADD, EDIT, DELETE, LIST, IMPORT, EXPORT.

Tabla 38.

Mandato	Sintaxis	Descripción	Ejemplo

Registrar nuevo usuario	`ADD [`*`nombreusuario`*
	`[| `*`dominio`*`\`*`nombreusuario`*`]]`
	`[/FORCED]`
		El distintivo /FORCED inhabilitará el botón Cancelar del asistente de forma que el registro finalizará satisfactoriamente. Si no se especifica el nombre de usuario, se utilizará el nombre de usuario actual.	`fprconsole add domain0\testuser`
			`fprconsole add testuser`
			`fprconsole add testuser /FORCED`

Editar usuario registrado	`EDIT [`*`nombreusuario`* `[| `*`dominio`*`\`*`nombreusuario`*`]]`	Si no se especifica el nombre de usuario, se utilizará el nombre de usuario actual. **Nota:** El usuario editado debe verificar primero su huella dactilar.	`fprconsole edit domain0\testuser` `fprconsole edit testuser`

Tabla 38. (continuación)

Mandato	Sintaxis	Descripción	Ejemplo

Suprima un usuario	`DELETE [`*`nombreusuario`* `[| `*`dominio`*`\`*`nombreusuario`* `| /ALL]]`	El distintivo /ALL borrará todos los usuarios registrados en este sistema. Si no se especifica el nombre de usuario, se utilizará el nombre de usuario actual.	`fprconsole delete domain0\testuser`
			`fprconsole delete testuser`
			`fprconsole delete /ALL`

Enumerar usuarios registrados	`List`		
Exportar usuario registrado a un archivo	`Sintaxis:` `EXPORT nombreusuario [| dominio\nombreusuario] archivo`	Este mandato exportará un usuario registrado a un archivo de la unidad de disco duro. A continuación, el usuario se puede importar utilizando el mandato IMPORT en otro sistema o en el mismo sistema si se suprime el usuario.	
Importar usuario registrado	`Sintaxis: IMPORT` *`archivo`*	La importación importará el usuario desde el archivo especificado. **Nota:** Si el usuario en el archivo ya está registrado en el mismo sistema utilizando las mismas huellas dactilares, no se garantiza qué usuario tendrá precedencia en la operación de identificación.	

Mandatos de valores globales

Los valores globales del Software de huellas dactilares se pueden cambiar mediante la sección SETTINGS. Todos los mandatos en esta sección necesitan derechos de administrador. La sintaxis es:

`FPRCONSOLE SETTINGS` *`mandato`*

donde *mandato* es uno de los mandatos siguientes: SECUREMODE, LOGON, CAD, TBX, SSO.

Tabla 39.

Mandato	Descripción	Sintaxis	Ejemplo
Modalidad de seguridad	Este valor conmuta entre las modalidades Cómoda y Segura del Software de huellas dactilares.	`SECUREMODE 0|1`	Para establecer la modalidad cómoda: `fprconsole settings securemode 0`

Tabla 39. (continuación)

Mandato	Descripción	Sintaxis	Ejemplo
Tipo de inicio de sesión	Este valor habilita (1) o inhabilita (0) la aplicación de inicio de sesión. Si se utiliza el parámetro /FUS, el inicio de sesión está habilitado en la modalidad de Conmutación rápida de usuario, si la configuración del sistema lo permite.	`LOGON 0|1 [/FUS]`	
CTRL+ALT+DEL mensaje	Este valor habilita (1) o inhabilita (0) el texto "Pulse CTRL+ALT+SUPR" en el inicio de sesión.	`CAD 0|1`	
Seguridad de encendido	Este valor desactiva globalmente (0) el soporte de la seguridad de encendido en el software de huellas dactilares. Cuando el soporte de seguridad de encendido está desactivado, no se muestra ningún asistente ni páginas de seguridad de encendido, y no importa cuáles son los valores del BIOS.	`TBX 0|1`	
Firma única de seguridad de encendido	Este valor habilita (1) o inhabilita (0) el uso de las huellas dactilares utilizado en el BIOS en el inicio de sesión para realizar automáticamente el inicio de sesión del usuario cuando se ha verificado el usuario en el BIOS.	`SSO 0|1`	

Modalidad segura y cómoda

El Software de huellas dactilares de ThinkVantage se puede ejecutar en dos modalidades seguras, una modalidad cómoda y una modalidad segura.

La modalidad cómoda está destinada a PC domésticos donde no sea tan importante un nivel de seguridad alto. Todos los usuarios pueden realizar todas las operaciones, incluidas la edición de pasaportes de otros usuarios y la posibilidad de iniciar sesión en el sistema utilizando contraseña (sin la autentificación de huellas dactilares).

La modalidad segura está destinada para las situaciones en las que desee conseguir mayor seguridad. Las funciones especiales están reservadas solamente a los administradores. Sólo los administradores puede iniciar sesión utilizando contraseñas, sin autentificación adicional.

Un *Administrador* es cualquier miembro del grupo de Administradores locales. Después de establecer la modalidad segura, sólo el administrador podrá conmutar de nuevo a la modalidad simple.

Modalidad segura – Administrador

En el Inicio de sesión, la modalidad segura visualiza el siguiente mensaje si se especifica el nombre de usuario o la contraseña incorrectos: ″Sólo los administradores pueden iniciar sesión en este sistema con el nombre de usuario y contraseña″. Esto se realiza para mejorar la seguridad y evitar proporcionar a los hackers información acerca de por qué no pueden iniciar la sesión.

Tabla 40.

Huellas dactilares	**Descripción**
Crear un nuevo pasaporte	Los administradores pueden crear su propio pasaporte y también pueden crear el pasaporte de un usuario con limitaciones.
Editar pasaportes	Los administradores pueden editar *sólo* su propio pasaporte.
Suprimir pasaporte	Los administradores pueden suprimir todos los pasaportes de usuarios con limitaciones y otros pasaportes de administrador. Si otros usuarios están utilizando la seguridad de encendido, el administrador tendrá la opción en este momento de eliminar las plantillas de usuario de la seguridad de encendido.
Seguridad de encendido	Los administradores pueden suprimir las huellas dactilares del usuario con limitaciones y del administrador utilizadas en el encendido. **Nota:** Debe haber como mínimo una huella dactilar presente cuando la modalidad de encendido está habilitada.
Valores	
Valores de inicio de sesión	Los administradores pueden realizar cambios en todos los valores de inicio de sesión.
Protector de pantalla protegido	Los administrador pueden acceder.
Tipo de pasaporte	Los administradores pueden acceder. Sólo importante con el servidor.
Modalidad de seguridad	Los administradores pueden conmutar entre la modalidad segura y la modalidad cómoda.
Servidores Pro	Los administradores pueden acceder. Sólo importante con el servidor.

Modalidad segura - Usuario con limitaciones

Durante un inicio de sesión de Windows, un usuario con limitaciones debe utilizar una huella dactilar para iniciar sesión. Si su lector de huellas dactilares no funciona, será necesario que un administrador cambie el valor del software de huellas dactilares a la modalidad cómoda para habilitar el acceso de nombre de usuario y contraseña.

Tabla 41.

Huellas dactilares	
Crear un nuevo pasaporte	El usuario con limitaciones no puede acceder.

Tabla 41. (continuación)

Huellas dactilares	
Editar pasaportes	El usuario con limitaciones puede editar sólo su propio pasaporte.
Suprimir pasaporte	El usuario con limitaciones puede borrar sólo su propio pasaporte.
Seguridad de encendido	El usuario con limitaciones no puede acceder.
Valores	
Valores de inicio de sesión	El usuario con limitaciones no puede modificar los valores de inicio de sesión.
Protector de pantalla protegido	El usuario con limitaciones puede acceder.
Tipo de pasaporte	El usuario con limitaciones no puede acceder.
Modalidad de seguridad	El usuario con limitaciones no puede modificar las modalidades de seguridad.
Servidores Pro	El usuario con limitaciones puede acceder - Sólo relevante con el servidor.

Modalidad cómoda - Administrador

Durante un inicio de sesión de Windows, los administradores puede iniciar sesión utilizando su propio nombre de usuario y contraseña o sus huellas dactilares.

Tabla 42.

Huellas dactilares	
Crear un nuevo pasaporte	Los administradores puede crear *sólo* su propio pasaporte.
Editar pasaportes	Los administradores pueden editar *sólo* su propio pasaporte.
Suprimir pasaporte	Los administradores pueden suprimir *sólo* su propio pasaporte.
Seguridad de encendido	Los administradores pueden suprimir las huellas dactilares del usuario con limitaciones y del administrador utilizadas en el encendido. **Nota:** Debe haber como mínimo una huella dactilar presente cuando la modalidad de encendido está habilitada.
Valores	
Valores de inicio de sesión	Los administradores pueden realizar cambios en todos los valores de inicio de sesión.
Protector de pantalla protegido	Los administradores pueden acceder.
Tipo de pasaporte	Los administradores pueden acceder. Sólo relevante con el servidor.
Modalidad de seguridad	Los administradores pueden conmutar entre la modalidad segura y la modalidad cómoda.

Tabla 42. (continuación)

Huellas dactilares	
Servidores Pro	Los administradores pueden acceder. Sólo importante con el servidor.

Modalidad cómoda - Usuario con limitaciones

Durante un inicio de sesión de Windows, los usuarios con limitaciones pueden iniciar sesión utilizando su propio nombre de usuario y contraseña o sus huellas dactilares.

Tabla 43.

Huellas dactilares	
Crear un nuevo pasaporte	Los usuarios con limitaciones pueden crear sólo su propia contraseña.
Editar pasaportes	Los usuarios con limitaciones pueden editar sólo su propio pasaporte
Suprimir pasaporte	Los usuarios con limitaciones pueden suprimir sólo su propio pasaporte.
Seguridad de encendido	Los usuarios con limitaciones pueden suprimir sólo sus propias huellas dactilares.
Valores	
Valores de inicio de sesión	Los usuarios con limitaciones no pueden modificar las valores de Inicio de sesión.
Protector de pantalla protegido	Los usuarios con limitaciones pueden acceder.
Tipo de pasaporte	Los usuarios con limitaciones pueden acceder. Sólo relevante con el servidor.
Modalidad de seguridad	Los usuarios con limitaciones no pueden modificar las modalidades de seguridad.
Servidores Pro	Los usuarios con limitaciones pueden acceder. Sólo relevante con el servidor.

Software de huellas dactilares de ThinkVantage y Novell Netware Client

Los nombres de usuario y las contraseñas del Software de huellas dactilares de ThinkVantage y de Novell deben coincidir.

Si tiene instalado en el sistema el Software de huellas dactilares de ThinkVantage y, a continuación, instala Novell Netware Client, es posible que algunos elementos del registro se sobregraben. Si se encuentra con problemas al iniciar la sesión del Software de huellas dactilares de ThinkVantage, vaya a la pantalla de los valores de Inicio de sesión y vuelva a habilitar el Protector de inicio de sesión.

Si tiene instalado en el sistema Novell Netware Client, pero no ha iniciado sesión en el cliente antes de instalar el Software de huellas dactilares de ThinkVantage, aparecerá la pantalla de Inicio de sesión de Novell. Proporcione la información solicitada por la pantalla.

Para cambiar los valores del Protector de inicio de sesión:

- Inicie el Centro de control.
- Pulse **Valores**
- Pulse **Valores de inicio de sesión**
- Habilite o inhabilite el Protector de inicio de sesión.

  Si desea utilizar el inicio de sesión de huellas dactilares, seleccione el recuadro Sustituir inicio de sesión de Windows por el inicio de sesión protegido mediante huellas dactilares. Tenga en cuenta que Habilitar o Inhabilitar el protector de inicio de sesión requiere el rearranque.
- Habilite o inhabilite la conmutación rápida de usuario, cuando el sistema lo permita.
- (Característica opcional) Habilite o inhabilite el inicio de sesión automático para un usuario autentificado mediante la seguridad de arranque de encendido.
- Establecer los valores de inicio de sesión de Novell. Los valores siguientes están disponibles al iniciar sesión en una red Novell:
  - **Activado**

    El Software de huellas dactilares de ThinkVantage proporciona automáticamente credenciales conocidas. Si el inicio de sesión de Novell falla, la pantalla de inicio de sesión de Novell Client se visualizará junto con un indicador de solicitud para especificar los datos correctos.
  - **Preguntar durante el inicio de sesión**

    El software de huellas dactilares de ThinkVantage visualiza la pantalla de inicio de sesión de Novell Client y un indicador de solicitud para especificar los datos de inicio de sesión.
  - El Software de huellas dactilares de

    ThinkVantage **inhabilitado** no intenta el inicio de sesión de Novell.

Apéndice A. Parámetros de la línea de mandatos para la instalación

Microsoft Windows Installer proporciona varias funciones de administrador mediante los parámetros de la línea de mandatos.

Procedimiento de instalación administrativa y parámetros de la línea de mandatos

Windows Installer puede realizar una instalación administrativa de una aplicación o de un producto en una red para que éste sea utilizado por un grupo de trabajo o para la personalización del mismo. Para el paquete de instalación de Rescue and Recovery, una instalación administrativa desempaqueta los archivos fuente de la instalación en una ubicación determinada.

- Para ejecutar una instalación administrativa, ejecute el paquete de instalación desde la línea de mandatos utilizando el parámetro /a:

  ```
  Setup.exe /a
  ```

Una instalación administrativa presenta un asistente que solicita al usuario administrativo que especifique las ubicaciones para desempaquetar los archivos de instalación. La ubicación de extracción por omisión es C:\. Puede seleccionar una nueva ubicación que puede incluir unidades que no sean C:\ (otras unidades locales, unidades de red correlacionadas, etc.). También puede crear nuevos directorios durante este paso.

- Para ejecutar una instalación administrativa de forma silenciosa, puede establecer la propiedad pública TARGETDIR en la línea de mandatos para especificar la ubicación de extracción:

  ```
  Setup.exe /s /v"/qn TARGETDIR=F:\IBMRR"
  ```

  O bien

  ```
  msiexec.exe /i "IBM Rescue and Recovery.msi" /qn TARGETDIR=F:\IBMRR
  ```

Después de completar una instalación administrativa, el administrador puede personalizar los archivos fuente, por ejemplo, añadiendo valores a TVT.TXT.

Utilización de MSIEXEC.EXE

: Para instalar a partir de las fuentes desempaquetadas después de realizar las personalizaciones, el usuario llama a MSIEXEC.EXE desde la línea de mandatos, pasando el nombre del archivo *.MSI desempaquetado. MSIEXEC.EXE es el programa ejecutable del Instalador utilizado para interpretar los paquetes de instalación e instalar los productos en sistemas de destino.

```
msiexec /i "C:\CarpetaWindows\Perfiles\NombreUsuario\
Personal\MisValores\nombre proyecto\configuración del producto\nombre del release\
DiskImages\Disk1\nombre del producto.msi"
```

Nota: Entre el mandato anterior en una única línea sin espacios a continuación de las barras inclinadas.

La Tabla 44 en la página 146 describe los parámetros de la línea de mandatos disponibles que se pueden utilizar con MSIEXEC.EXE, así como ejemplos de cómo utilizarlos.

Tabla 44. parámetros de la línea de mandatos

Parámetro	Descripción

/I *paquete*
o bien
código del producto
	Utilice este formato para instalar el producto:
	`Othello:msiexec /i "C:\`*`CarpetaWindows`*`\Perfiles\`
	`NombreUsuario``\Personal\MisValores`
	`\Othello\Versión de prueba\`
	`Release\ImágenesDisco\Disco1\`
	`Othello Beta.msi"`
	
	El código del producto se refiere a la GUI que se genera automáticamente en la propiedad del código del producto de la vista de proyectos del producto.

/a *paquete*	La opción **/a** permite a los usuarios con privilegios de administrador instalar un producto en la red.
/x *paquete* o *código del producto*	La opción **/x** desinstala un producto.
/L [i|w|e|a|r|u|c|m|p|v|+] *archivo de registro*	La creación con la opción **/L** especifica la vía de acceso al archivo de registro; estos distintivos indican qué información se debe registrar en el archivo de registro: • **i** registra mensajes d estado • **w** registra mensajes de aviso no críticos • **e** registra cualquier mensaje de error • **a** registra el inicio de las secuencias de acción • **r** registra registros específicos de las acciones • **u** registra solicitudes de usuario • **c** registra parámetros iniciales de la interfaz de usuario • **m** registra mensajes de falta de memoria • **p** registra valores de terminal • **v** registra el valor de salida detallada • **+** se añade a un archivo existente • * es un carácter comodín que le permite registrar toda la información (excluido el valor de salida detallada)
/q [n|b|r|f]	La opción /q se utiliza para establecer el nivel de interfaz de usuario conjuntamente con los distintivos siguientes: • **q** o qn no crea ninguna interfaz de usuario • **qb** crea una interfaz de usuario básica Los siguientes valores de la interfaz de usuario visualizan un cuadro de diálogo modal al final de la instalación: • **qr** visualiza una interfaz de usuario reducida • **qf** visualiza una interfaz de usuario completa • **qn+** no visualiza ninguna interfaz de usuario • **qb+** visualiza una interfaz de usuario básica
/? o /h	Ambos mandatos visualizan la información de copyright de Windows Installer

Tabla 44. parámetros de la línea de mandatos (continuación)

Parámetro	Descripción

TRANSFORMS	Utilice el parámetro **TRANSFORMS** de la línea de mandatos para especificar cualquier transformación que le gustaría aplicar al paquete base. La llamada de la línea de mandatos a la transformación puede tener un aspecto similar al siguiente:
	`msiexec /i "C:\CarpetasWindows\`
	`Perfiles\NombreUsuario\Personal`
	`\MisValores\`
	`El nombre de proyecto\Versión de prueba\`
	`Mi Release-1`
	`\DiskImages\Disk1\`
	`NombreProducto.msi"`
	`TRANSFORMS="Nueva transformación 1.mst"`
	
	Puede separar varias transformaciones mediante un punto y coma. Debido a esto, se recomienda que no utilice punto y coma en el nombre de la transformación, ya que el servicio de Windows Installer lo interpretará incorrectamente.

Propiedades	Todas las propiedades públicas se pueden establecer o modificar desde la línea de mandatos. Las propiedades públicas se distinguen de las propiedades privadas por el hecho de que están todas en mayúsculas. Por ejemplo, *COMPANYNAME* es una propiedad pública.
	
	Para establecer una propiedad en la línea de mandatos, utilice la sintaxis siguiente:
	`PROPERTY=VALUE`
	
	Si deseara cambiar el valor de *COMPANYNAME*, especificaría lo siguiente:
	`msiexec /i "C:\CarpetaWindows\`
	`Perfiles\NombreUsuario\Personal`
	`\`
	`MisValores\El nombre de proyecto\`
	`Versión de prueba\Mi release-1`
	`\`
	`DiskImages\Disk1\NombreProducto.msi"`
	`COMPANYNAME="InstallShield"`

Apéndice B. Parámetros y valores de TVT.TXT

Los siguientes valores por omisión son los parámetros que se sugieren. Los parámetros pueden diferir para configuraciones distintas, versión precargada, descargada de la Web u OEM. Están disponibles los siguientes parámetros de configuración de la instalación:

Tabla 45. Valores de TVT.TXT

Parámetro	**Valores**
AccessFile (vea GUIGroup)	*nombrearchivo*, donde *nombrearchivo* es la vía de acceso calificada totalmente de un archivo que contiene los nombres de los grupos locales (no grupos de dominio) de Windows a los que se permite realizar operaciones de Rescue and Recovery. Si está vacío o falta, todos los usuarios que puedan iniciar sesión en el sistema podrán iniciar la GUI y realizar operaciones de la línea de mandatos. Por omisión, el archivo está vacío.
BackupPartition	0 = Primera partición de una unidad especificada 1 = Segunda partición de una unidad especificada 2 = Tercera partición de una unidad especificada 3 = Cuarta partición de una unidad especificada Las unidades se especifican en las secciones siguientes: [BackupDisk] = unidad de disco duro local [SecondDisk] = segunda unidad de disco duro local [USBDisk] = unidad de disco duro USB **Nota:** Las particiones ya deben existir. Si no está establecidas, se solicitará al usuario que establezca la partición (si hay más de una partición en la unidad de destino cuando se seleccione la unidad de destino en la interfaz del usuario).
BatteryPercentRequired	El rango es de 0 a 100. El valor por omisión es 100.
CPUPriority	*n* donde *n* = de 1 a 5; 1 es la prioridad más baja y 5 la prioridad más alta. El valor por omisión es 3.
CustomPartitions -	0 = Realizar copia de seguridad de todas las particiones 1 = Buscar IncludeInBackup en cada partición
DisableAnalyze	0 = Mostrar la opción Optimizar almacenamiento de copia de seguridad 1 = Ocultar esta opción El valor por omisión es 0.
DisableArchive	0 = Habilitar archivado 1 = Ocultar archivado El valor por omisión es 0.

Tabla 45. Valores de TVT.TXT (continuación)

Parámetro	Valores
DisableBackupLocation	0 = Habilitar todo el destino 0x01 = Inhabilitar destino local 0x02 = Inhabilitar unidad de CD/DVD 0x08 = Inhabilitar unidad de disco duro USB 0x10 = Inhabilitar red 0x20 = Inhabilitar segunda unidad de disco duro 1 = Ocultar archivado Estas opciones se pueden combinar para inhabilitar varias ubicaciones. Por ejemplo, un valor de 0x0A inhabilitaría la unidad de CD/DVD y de disco duro USB; un valor de 0x38 inhabilitaría la unidad de disco duro USB, la red y la segunda unidad de disco duro. Para habilitar sólo la copia de seguridad en la unidad de disco duro local, puede utilizar 0x3A (o incluso 0xFE).
DisableBootDisc	0 = Crear CD arrancable al crear copias de seguridad en CD/DVD 1 = No crear CD arrancable La función Disable Boot Disc es sólo para copias de seguridad, no para archivado.
DisableDelete	0 = Mostrar la opción de suprimir copias de seguridad 1 = Ocultar esta opción El valor por omisión es 0.
DisableExclude	0 = Mostrar la opción de excluir archivo/carpetas 1 = Ocultar la opción de excluir archivo/carpetas El valor por omisión es 0.
DisableLiveUpdate	0 = Mostrar la opción LiveUpdate 1 = Ocultar esta opción El valor por omisión es 0.
DisableMigrate	0 = Mostrar Crear archivo de migración desde copia de seguridad 1 = Ocultar esta opción El valor por omisión es 0.
DisableRestore	0 = Habilitar Restaurar 1 = Ocultar Restaurar El valor por omisión es 0.

Tabla 45. Valores de TVT.TXT (continuación)

Parámetro	Valores
DisableSchedule	0 = Mostrar la opción Planificación de copia de seguridad 1 = Ocultar opción Planificación de copia de seguridad El valor por omisión es 0.
DisableSFR	0 = Habilitar Restaurar un único archivo 1 = Ocultar Restaurar un único archivo El valor por omisión es 0.
DisableSingleStorage	0 = Mostrar opción Almacenamiento único 1 = Ocultar esta opción El valor por omisión es 0.
DisableViewBackups	0 = Mostrar opción Visualizar copias de seguridad 1 = Ocultar esta opción El valor por omisión es 0.
DisableVerifyDisc	0 = Verificar operaciones de grabación óptica 1 = No verificar operaciones de grabación óptica El valor por omisión es 0.
Exclude (vea Include)	0 = No aplicar GUIEXCLD.TXT 1 = Aplicar GUIEXCLD.TXT.txt **Notas:** 1. La exclusión e inclusión de archivos se puede definir antes de la instalación y se puede aplicar durante el proceso de instalación. 2. Exclude e Include no tener ambos el valor de 1.
GUIGroup (vea AccessFile)	*group*, donde *group* es un grupo local de Windows (no un grupo de dominio) al que se permite realizar operaciones de Rescue and Recovery. La lista de grupos con privilegios se almacena en un archivo definido en la entrada AccessFile.
HideAdminBackups	0 = Mostrar copias de seguridad de administrador en lista. 1 = Ocultar copias de seguridad de administrador. El valor por omisión es 0.
HideBaseFromDelete	0 = Mostrar copia de seguridad base en dialogo Suprimir copias de seguridad. 1 = Ocultar copia de seguridad base en diálogo Suprimir copias de seguridad. El valor por omisión es 0.
HideBootUSBDialog	0 = Mostrar indicador si se está realizando copia de seguridad en una unidad de disco duro USB y no es arrancable 1 = Ocultar indicador El valor por omisión es 0.

Tabla 45. Valores de TVT.TXT (continuación)

Parámetro	Valores
HideDiffFileSystems	0 = Mostrar particiones FAT/FAT32 al restaurar/guardar archivos 1 = Ocultar particiones FAT/FAT32 al restaurar/guardar archivos El valor por omisión es 0.
HideCSSEncrypt	0 = No ocultar Cifrar copias de seguridad utilizando Client Security Solution 1 = Ocultar Cifrar copias de seguridad utilizando Client Security Solution El valor por omisión es 0.
HideGUI	0 = Mostrar la GUI a usuarios autorizados 1 = Ocultar la GUI a todos los usuarios
HideLocationNotFoundMessage	0 = Mostrar mensaje de diálogo 1 = Ocultar mensaje de diálogo El valor por omisión es 0.
HideLockHardDisk	0 = Mostrar la opción Proteger disco duro de corrupción MBR 1 = Ocultar esta opción El valor por omisión es 1.
HideMissedBackupMessages	0 = Ocultar recuadro de diálogo 1 = Ocultar recuadro de diálogo El valor por omisión es 1.
HideNoBatteryMessage	0 = Mostrar mensaje 1 = Ocultar mensaje El valor por omisión es 1.
HideNumBackupsDialog	0 = No ocultar el diálogo que muestra al usuario cuando ha alcanzado el número máximo de copias de seguridad 1 = Ocultar el diálogo que muestra al usuario cuando ha alcanzado el número máximo de copias de seguridad El valor por omisión es 1.
HidePowerLossBackupMessage	0 = Mostrar mensaje de pérdida de alimentación con copia de seguridad 1 = Ocultar mensaje El valor por omisión es 0.
HidePasswordPersistence	0 = Ocultar la GUI 1 = Mostrar la GUI El valor por omisión es 0.

Tabla 45. Valores de TVT.TXT (continuación)

Parámetro	Valores
HidePasswordProtect	0 = Mostrar recuadro de selección Proteger mediante contraseña. 1 = Ocultar recuadro de selección Proteger mediante contraseña. El valor por omisión es 0.
HideSuspendCheck	0 = No ocultar el recuadro de selección Activar el sistema desde suspensión/hibernación 1 = Ocultar recuadro de selección El valor por omisión es 1.
Include (vea Exclude)	0 = No aplicar GUIINCLD.TXT 1 = Aplicar GUIINCLD.TXT y visualizar la opción para establecer la inclusión de archivos y carpetas **Notas:** 1. La exclusión y selección de archivos se puede definir antes de la instalación y se puede aplicar durante el proceso de instalación. 2. Exclude e Include no tener ambos el valor de 1.
LocalBackup2Location	*x**nombrecarpeta* donde *x* = letra de la unidad y *nombrecarpeta* es el nombre de carpeta totalmente calificado.) El valor por omisión es el siguiente: *primera letra de la partición en la segunda unidad*:\IBMBackupData **Notas:** 1. Debido a que la letra de la unidad puede cambiar con el tiempo, Rescue and Recovery asociará la letra de la unidad a una partición en el momento de la instalación y, a continuación, utilizará la información de la partición en lugar de la letra de la unidad. 2. Éste es el campo de la ubicación de la entrada `TaskParameters`.
LockHardDisk	0 = No bloquear el disco duro para proteger el MBR 1 = Bloquear el disco duro El valor por omisión es 0.
MaxBackupSizeEnforced	*x*, donde *x* es el tamaño en GB. Este valor no impedirá que una copia de seguridad exceda este umbral. Sin embargo, si se excede el umbral, se avisará al usuario acerca del tamaño del archivo la próxima vez que se realice una copia de seguridad ″Bajo demanda″. El valor por omisión es 0.
MaxNumberOf IncrementalBackups	Valor por omisión = 5, mín = 2, máx = 32
MinAnalyzeFileSize *n*	Donde *n* es el tamaño mínimo del archivo en MB para visualizar un archivo al usuario en la pantalla ″Optimizar espacio de almacenamiento de copia de seguridad″. El valor por omisión es 20

Tabla 45. Valores de TVT.TXT (continuación)

Parámetro	Valores
NetworkUNCPath	Compartición de red con el formato: *nombresistema**carpetacompartición* No hay ningún valor por omisión. **Nota:** Esta ubicación no estará protegida por el Controlador del filtro de archivos.
NetworkUNCPath	*nombre compartición servidor*, por ejemplo, \\MISERVIDOR\COMPARTICIÓN\CARPETA
NumMinutes	*x*, donde la tarea se ejecuta después de que hayan transcurrido *x* minutos.
PasswordRequired	0 = No es necesaria ninguna contraseña para abrir el entorno de Rescue and Recovery. 1 = Contraseña necesaria para abrir el entorno de Rescue and Recovery.
PDAPreRestore	*cmd*, donde *cmd* es una vía de acceso calificada totalmente del programa que se ejecutará en el entorno de Rescue and Recovery antes de la operación de restauración.
PDAPreRestore *n*	*cmd*, donde *cmd* es una vía de acceso calificada totalmente del programa que se ejecutará en el entorno de Rescue and Recovery antes de la operación de restauración.
PDAPreRestoreParameters	Parámetros que se utilizarán en el programa PDARestore.
PDAPreRestoreParameters *n*	Parámetros que se utilizarán en el programa PDARestore.
PDAPreRestoreShow	0 = Ocultar tarea 1 = Mostrar tarea
PDAPreRestoreShow *n*	0 = Ocultar tarea 1 = Mostrar tarea
PDAPostRestore	*cmd*, donde *cmd* es una vía de acceso calificada totalmente del programa que se ejecutará en el entorno de Rescue and Recovery antes de la operación de restauración.
PDAPostRestore *n*	*cmd*, donde *cmd* es una vía de acceso calificada totalmente del programa que se ejecutará en el entorno de Rescue and Recovery antes de la operación de restauración.
PDAPostRestoreParameters	Parámetros que se utilizarán en el programa PDARestore.
PDAPostRestoreParameters *n*	Parámetros que se utilizarán en el programa PDARestore.
PDAPostRestoreShow	0 = Ocultar tarea 1 = Mostrar tarea
PDAPostRestoreShow *n*	0 = Ocultar tarea 1 = Mostrar tarea
Post (vea PostParameters)	*cmd*, donde *cmd* es una vía de acceso calificada totalmente del archivo ejecutable que se ejecutará después de la tarea primaria.

Tabla 45. Valores de TVT.TXT (continuación)

Parámetro	Valores
Post (vea PostParameters) *n*	Donde *n* es el número de copia de seguridad 0, 1, 2, 3...32 *cmd*, donde *cmd* es una vía de acceso calificada totalmente del archivo ejecutable que se ejecutará después de la tarea primaria. Por ejemplo: • Post0=command.bat *vía de acceso* Se ejecuta después de la copia de seguridad base • Post1=command.bat *vía de acceso* Se ejecuta después de la copia de seguridad incremental **Nota:** Es sólo para copia de seguridad
PostParameters (vea Post)	*cmd*, donde *cmd* es una vía de acceso calificada totalmente del archivo ejecutable que se ejecutará después de la tarea primaria. Es sólo para copia de seguridad.
PostParameters *n* (vea Post)	*parámetros*, donde *parámetros* son los parámetros que se utilizarán en la post-tarea.
	parámetros, donde *parámetros* son los parámetros que se utilizarán en la post-tarea. **Nota:** Es sólo para copia de seguridad
PostRestore	*cmd*, donde *cmd* es un vía de acceso calificada totalmente del programa que se ejecutará en Windows después de que se haya completado la operación de restauración
PostRestore *n*	*cmd*, donde *cmd* es un vía de acceso calificada totalmente del programa que se ejecutará en Windows después de que se haya completado la operación de restauración.
PostRestoreParameters	Parámetros que se utilizarán en el programa PostRestore
PostRestoreParameters *n*	Parámetros que se utilizarán en el programa PostRestore
PostRestoreShow	0 = Ocultar tarea Restaurar 1 = Mostrar tarea Restaurar
PostRestoreShow *n*	0 = Ocultar tarea Restaurar 1 = Mostrar tarea Restaurar
PostShow	0 = Ocultar post-tarea 1 = Mostrar post-tarea El valor por omisión es 0.
PostShow *n*	0 = Ocultar post-tarea 1 = Mostrar post-tarea El valor por omisión es 0. Donde *n* es el número de copia de seguridad 0, 1, 2, 3....32 **Nota:** Es sólo para copia de seguridad
Pre (vea PreParameters)	*cmd*, donde *cmd* es una vía de acceso calificada totalmente del archivo ejecutable que se ejecutará antes de la tarea primaria.

Tabla 45. Valores de TVT.TXT (continuación)

Parámetro	Valores
Pre (vea PreParameters) *n*	Donde *n* es el número de copia de seguridad 0, 1, 2, 3....32 *cmd*, donde *cmd* es una vía de acceso calificada totalmente del archivo ejecutable que se ejecutará antes de la tarea primaria. Por ejemplo: • Pre0=command.bat *vía de acceso* Se ejecuta antes de la copia de seguridad base • Pre1=command.bat *vía de acceso* Se ejecuta antes de la copia de seguridad incremental **Nota:** Es sólo para copia de seguridad.
PreParameters (vea Pre)	Donde *parámetros* son los parámetros que se utilizarán en la pre-tarea.
PreRejuvenate *cmd*	Donde *cmd* es la vía de acceso calificada totalmente al programa que se ejecutará en Windows antes de una operación de rejuvenecimiento
PreRejuvenateParameters *parámetros*	Donde *parámetros* son los parámetros que se utilizarán en el programa PreRejuvenate.
PreRejuvenateShow	0 = Ocultar tarea 1 = Mostrar tarea
PostRejuvenate *cmd*	*cmd*, donde *cmd* es la vía de acceso calificada totalmente del programa que se ejecutará en Windows después de una operación de rejuvenecimiento
PostRejuvenateParameters *parámetros*	Donde *parámetros* son los parámetros que se utilizarán en el programa PostRejuvenate.
PostRejuvenateShow	0 = Ocultar tarea 1 = Mostrar tarea
PreShow	0 = Ocultar pre-tarea 1 = Mostrar pre-tarea El valor por omisión es 1.
PreShow *n*	Donde *n* es el número de copia de seguridad 0, 1, 2, 3....32 *cmd*, donde *cmd* es una vía de acceso calificada totalmente del archivo ejecutable que se ejecutará antes de la tarea primaria. **Nota:** Es sólo para copia de seguridad
PreWinRestore	*cmd*, donde *cmd* es una vía de acceso calificada totalmente del programa que se ejecutará en Windows antes de una operación de restauración.
PreWinRestore *n*	*cmd*, donde *cmd* es una vía de acceso calificada totalmente del programa que se ejecutará en Windows antes de una operación de restauración.
PreWinRestoreParameters	Parámetros que se utilizarán en el programa PreWinRestore
PreWinRestoreParameters *n*	Parámetros que se utilizarán en el programa PreWinRestore
PreWinRestoreShow	0 = Ocultar post-tarea 1 = Mostrar post-tarea

Tabla 45. Valores de TVT.TXT (continuación)

Parámetro	Valores
PreWinRestoreShow *n*	0 = Ocultar post-tarea 1 = Mostrar post-tarea
ResumePowerLossBackup	0 = No reanudar el proceso de copia de seguridad si se ha perdido la alimentación en medio de la última copia de seguridad 1 = Reanudar la copia de seguridad El valor por omisión es 1.
RunBaseBackup	0 = No realizar la copia de seguridad base 1 = Realizar la copia de seguridad base El valor por omisión es 0. `runbasebackuplocation=(`*`Ubicación`*`)` Los valores son: L = Local U = USB N = Red S = Segunda unidad de disco duro C = CD
ScheduleDayOfTheMonth	*x*, donde *x* es igual a un valor de 1 a 28 o 35 sólo para copias de seguridad mensuales. 35 = el último día del mes
ScheduleDayOfTheWeek	Sólo para copias de seguridad semanales 0 = Domingo 1 = Lunes 2 = Martes 3 = Miércoles 4 = Jueves 5 = Viernes 6 = Sábado El valor por omisión es 0 (domingo).
ScheduleFrequency	0 = No planificado 1 = Diariamente 2 = Semanalmente 3 = Mensualmente El valor por omisión es 2 (semanalmente).

Tabla 45. Valores de TVT.TXT (continuación)

Parámetro	Valores
ScheduleHour	*x*, donde *x* equivale a un valor de 0 a 23 y 0 es 12:00 AM, 12 es mediodía, y 23 son las 11:00 PM. El valor por omisión es 0.
ScheduleMinute	*x*, donde *x* equivale a un valor de 0 a 59 (que aumenta), que representa el minuto de la hora que se iniciará la copia de seguridad incremental. El valor por omisión es 0.
ScheduleWakeForBackup	0 = No activar el sistema para las copias de seguridad planificadas 1 = Activar el sistema, si es un sistema de sobremesa para copias de seguridad planificadas, pero no activar sistemas portátiles 2 = Activar el sistema independientemente de si se trata de un sistema de sobremesa o de un portátil El valor por omisión es 2. **Nota:** Si se activa un portátil para una copia de seguridad, pero no se detecta la alimentación de CA, volverá a la suspensión/hibernación antes de una operación de copia de seguridad.
ScheduleMode	*x*, donde *x* es una máscara de bits con un valor de: • 0 = Ninguna planificación • 0x01 = Cada minuto • 0x04 = Cada semana • 0x08 = Cada mes • 0x10 = Cada vez que se inicia el servicio (normalmente cada arranque de máquina) • 0x20 = La máquina se activa desde la suspensión/hibernación • 0x40 = Se conecta la unidad de disco duro USB • 0x80 = Se conecta la red • 0x100 = Se desconecta la red • 0x200 = Restablecimiento de contraseña de BIOS • 0x400 = Sustitución de placa madre Este parámetro se actualiza automáticamente cuando el usuario cambia los valores de la GUI. Si el valor ScheduleFrequency se cambia ya sea realizando los cambios manualmente en el archivo TVT.TXT o mediante script, reloadsched actualizará este parámetro. **Nota:** No es necesario establecer los bits de `Se conecta la unidad de disco duro USB` o `se conecta la red` para la sincronización automática de copias de seguridad desde la unidad de disco duro local a la unidad de disco duro USB o a la red.)
SkipLockedFiles	0 = Visualizar recuadro de diálogo cuando se encuentre un archivo bloqueado o corrupto 1 = Omitir siempre archivos bloqueados y corruptos

Tabla 45. Valores de TVT.TXT (continuación)

Parámetro	Valores
SPBackupLocation=2	Utilizado para establecer la copia de seguridad de la Partición de servicio. Si no se utiliza este valor, la Partición de servicio por omisión de 500 MB se restaurará cuando se elimine el CD de arranque, el CD de restauración y otros datos de la Partición de servicio.
Task	*cmd*, donde *cmd* es una vía de acceso calificada totalmente del programa que se ejecutará como la tarea primaria. **Nota:** El número de tareas no puede ser más de 50.
TaskParameter	*parámetros* son parámetros que se utilizarán en la tarea.
TaskShow	0 = Ocultar tarea 1 = Mostrar tarea El valor por omisión es 0.
UUIDMatchRequired	0 = No es necesaria la coincidencia de UUID del sistema. 1 = Es necesaria la coincidencia de UUID del sistema. **Nota:** Las copias de seguridad que se han capturado cuando UUIDMatchRequired estaba establecido en 1 continuarán necesitando una coincidencia de UUID, incluso si este valor se cambia posteriormente.
Yield	*n* donde *n* equivale a un valor de 0 a 8; 0 significa que Rescue and Recovery no cede prioridad y 8 significa queRescue and Recovery produce el valor máximo de prioridad. **Nota:** Una prioridad alta reducirá considerablemente el rendimiento de copia de seguridad y proporcionará un mejor rendimiento interactivo. El valor por omisión es 0.

Después de instalar Rescue and Recovery, se pueden modificar las siguientes configuraciones en el archivo TVT.TXT que está ubicado en el directorio de instalación. Se iniciarán con los valores asignados durante la instalación.

Copia de seguridad y restauración de TVT.txt

Para dar soporte a la instalación silenciosa, la configuración de Copia de seguridad y restauración de Rescue and Recovery está definida por un archivo externo (*TVT.TXT*) que se edita antes de la instalación. El archivo TVT.TXT seguirá el formato estándar del archivo .ini de Windows, con los datos organizados por secciones indicadas por [] y una entrada por línea con el formato “setting=valor”. Rescue and Recovery utilizarán el nombre del producto para la cabecera de sección (como por ejemplo Rapid Restore Ultra). Además, el archivo de filtro de inclusión/exclusión se puede definir antes de la instalación y se puede aplicar durante el proceso de instalación.

Si el administrador de TI desea personalizar sus copias de seguridad con valores, debe editar el archivo txt.txt en el directorio de instalación. El mejor momento para hacer esto es antes de instalar Rescue and Recovery o después de instalarlo y antes de realizar la primera copia de seguridad. Se incluye un archivo TVT.TXT en cada ubicación de copia de seguridad. Antes de realizar la primera copia de seguridad, existe solamente un archivo TVT.TXT. Si se utiliza este enfoque, todas las copias de

seguridad tendrán todos los cambios sin tener ninguno de los problemas de sincronización y de versión de TVT.TXT. Algunas veces se debe editar el archivo TVT.TXT después de una copia de seguridad. En este caso, existen dos formas de actualizar todos los archivos TVT.TXT con los cambios más recientes. El administrador de TI puede copiar el archivo TVT.TXT del directorio de instalación en las carpetas de copia de seguridad o iniciar otra copia de seguridad y el proceso sincronizará automáticamente todas las versiones de TVT.TXT con la versión del directorio de instalación. Es preferible el segundo método.

Planificación de copias de seguridad y tareas relacionadas

El planificador no está diseñado para ser específico de Rescue and Recovery. Sin embargo, la configuración se almacena en el mismo archivo TVT.TXT. Cuando esté instalado Rescue and Recovery, rellenará el planificador con los valores adecuados.

A continuación se muestra una descripción de la estructura del planificador:
- Ubicación: Carpeta de instalación
- Entrada para cada trabajo planificado
- Script que se debe ejecutar
- Conexión con nombre que se debe utilizar para las notificaciones de progreso. Esto es opcional.
- Información de planificación mensual, semanal, diaria, día laborable, fin de semana - múltiples planificaciones; por ejemplo, se puede dar soporte a martes y viernes, creando dos planificaciones
- Variables que se pasarán a las funciones

Tenga en cuenta el ejemplo siguiente: En el caso de que Rescue and Recovery realice una copia de seguridad incremental planificada, con devoluciones de llamada antes y después de la copia de seguridad, la siguiente entrada indica a la aplicación en función de ello:

```
[SCHEDULER]
Task1=rescuerecovery
[rescuerecovery]
Task="c:\program
files\ibm\Rescue and Recovery\
rrcmd.exebackup.bat"
TaskParameters=BACKUP
location=L name="Scheduled"
ScheduleFrequency=2
ScheduleDayOfTheMonth=31
ScheduleDayOfTheWeek=2
ScheduleHour=20
ScheduleMinute=0
ScheduleWakeForBackup=0
Pre="c:\Archivos de programa\antivirus\scan.exe"
Post="c:\Archivos de programa\logger\log.bat"
```

Gestión de diferentes archivos TVT.txt

Debido a que las unidades de disco duro tienen múltiples particiones, el programa de copia de seguridad y restauración necesita saber qué partición almacenará los datos de copia de seguridad. Si un destino determinado tiene múltiples particiones y se crearán scripts de las operaciones de copia de seguridad, es necesario

configurar el siguiente valor antes de la operación de copia de seguridad. Si el usuario puede inicializar la operación de copia de seguridad, puede omitir esta sección.

Para copias de seguridad de la unidad de disco duro local, el valor de configuración se encuentra en la sección BackupDisk del archivo TVT.TXT. Las copias de seguridad de la segunda unidad de disco duro utilizan la sección SecondDisk y las copias de seguridad de la unidad de disco duro USB utilizarían la sección USBDisk, de la forma siguiente:

```
BackupPartition=x
```

donde *x* es un rango de 0 - 3, donde 0 representa la primera partición de la unidad adecuada).

Nota: Las particiones ya deben existir. Si no está establecida, se solicitará al usuario, si hay más de una partición, cuando se seleccione el destino adecuado en la GUI. Por ejemplo: si se quisiera realizar una copia de seguridad de la segunda partición de la unidad de disco duro USB, la entrada del archivo TVT.TXT tendría el aspecto siguiente:

```
[USBDisk]
BackupPartition=1
```

Correlación de una unidad de red para copias de seguridad

La función de correlacionar unidad de red se basa en el archivo MAPDRV.INI que está ubicado en el directorio C:\Archivos de programa\IBM ThinkVantage\Common\MND. Toda la información se almacena en la sección DriveInfo.

La entrada Universal Naming Convention contiene el nombre del sistema y compartición de la ubicación a la que está intentando conectarse.

La entrada NetPath es la salida del archivo mapdrv.exe. Contiene el nombre real que se utilizó al realizar la conexión.

Las entradas User y Pwd contienen las entradas del nombre de usuario y contraseña. Estos están cifrados.

Lo siguiente es una entrada de ejemplo para correlacionar una unidad de red:

```
[DriveInfo]
UNC=\\server\share
NetPath=\\9.88.77.66\share
User=116226064151192077230149185054220105210064012092037082020l5...
Pwd=116226064151000000000149185054220105210064012092037082020l5...
```

Para el despliegue, este archivo se puede copiar en múltiples sistemas que utilizarán el mismo nombre de usuario y la misma contraseña. Rapid Restore Ultra sobregraba la entrada UNC de acuerdo con un valor en el archivo TVT.TXT.

Configuración de cuentas de usuario para copias de seguridad de red

Cuando se cree el directorio RRBACKUPS en la compartición de red, el servicio hace del directorio una carpeta de sólo lectura, y le asigna derechos de acceso de forma que *sólo* la cuenta que ha creado la carpeta tiene control total sobre la carpeta.

Para completar la operación de fusión, existen permisos MOVE para la cuenta de usuario. Si se ha iniciado sesión con una cuenta distinta que la cuenta que ha creado la carpeta inicialmente, como por ejemplo el administrador, el proceso de fusión fallará.

Apéndice C. Herramientas de la línea de mandatos

Los administradores de TI de la empresa también pueden invocar las funciones de Tecnologías ThinkVantage de forma local o remota mediante la interfaz de la línea de mandatos. Los valores de configuración se pueden mantener mediante valores del archivo de texto remoto.

Antidote Delivery Manager

Mailman

Utiliza el mandato C:\Archivos de programa|IBM ThinkVantage\Rescue and Recovery\ADM\mailman.exe. Este programa comprobará el Depósito de antídotos para ver si hay tareas en ejecución. No existen argumentos de la línea de mandatos.

Asistente de antídotos

Este mandato, AWizard.exe, se ubica donde el administrador lo instala. No existen argumentos de la línea de mandatos.

Establecer contraseñas

Para ver una descripción de las contraseñas, consulte “Contraseñas” en la página 37.

CFGMOD

CFGMOD proporciona un método para actualizar el archivo TVT.TXT mediante un script. El mandato CFGMOD se puede encontrar en el directorio C:\Archivos de programa\IBM ThinkVantage\Rescue and Recovery\. Si modifica la planificación de copia de seguridad, este mandato debe ir seguido de RELOADSCHED. Este programa de utilidad se debe ejecutar con privilegios de administrador.

Sintaxis:

```
cfgmod TVT.TXT archivo mod
```

El formato del archivo mod file requiere una línea por entrada. Cada entrada incluye un número de sección (delimitado por [y]), seguido por un nombre de parámetro, seguido por "=", seguido por el valor. Por ejemplo, para ajustar la planificación de copia de seguridad, las entradas del archivo mod podrían ser las siguientes:

```
[rescuerecovery]ScheduleFrequency=1
[rescuerecovery]ScheduleHour=8
[rescuerecovery]ScheduleMinute=0
```

Client Security Solution

Client Security Solution contiene las siguientes herramientas de la línea de mandatos:

SafeGuard PrivateDisk

La interfaz de la línea de mandatos está ubicada en la carpeta C:\Archivos de programa\IBM ThinkVantage\SafeGuard PrivateDisk\. La sintaxis es:

```
PDCMD
 [ADDCERT nombreVolumen /pw contraseñaAdmin /sn SNcert [/acc access]]  |
 [LIST]  |
 [MOUNT nombreVolumen [/pw contraseñaUsuario [/pt modalidadAuten]] [/ro]]  |
 [NEW nombreVolumen [/sz tamaño] [/dl letraUnidad] [/fs filesystem]
   [/pw contraseñaAdmin] [/pwu contraseñaUsuario]]  |
 [UNMOUNT nombreVolumen /f]  |
 [UNMOUNTALL [/f]]  |
 [SETPASSWORD nombreVolumen /pw contraseñaAdmin /pwu contraseñaUsuario [/ro]]
```

Los parámetros se muestran en la Tabla 46:

Tabla 46.

Parámetro	**Resultado**
ADDCDERT	Añade certificado al volumen PrivateDisk
LIST	Listar volúmenes PrivateDisk para este usuario
MOUNT	Monta un volumen PrivateDisk específico
NEW	Crea un nuevo volumen PrivateDisk
UNMOUNT	Desmonta un volumen PrivateDisk determinado
UNMOUNTALL	Desmonta todos los volúmenes PrivateDisk
SETPASSWORD	Establece contraseña de usuario en un volumen PrivateDisk
volumename	Nombre del archivo que contiene los archivos PrivateDisk
pw	Contraseña
sn	Número de serie del certificado.
acc	Tipo de acceso del certificado que se debe añadir. Los valores válidos son: • **adm** acceso de administrador • **uro** acceso de sólo lectura de usuario • **usr** acceso de grabación de usuario (valor por omisión)
pt	Método de autentificación. Los valores válidos son: • **0** Acceso de administrador (valor por omisión) • **1** Contraseña de usuario • **2** PIN para un inicio de sesión basado en certificado
ro	Sólo de lectura

Tabla 46. (continuación)

Parámetro	Resultado
sz	Tamaño (en Kbytes)
dl	Letra de la unidad para el volumen PrivateDisk (valor por omisión=siguiente letra de unidad disponible)
fs	Sistema de archivos. Los valores por omisión son: • FAT (valor por omisión) • NTFS
pwu	Contraseña de usuario
f	Forzar operación

Security Advisor

Para ejecutarlo desde la GUI, pulse **Inicio->Programas->ThinkVantage->Client Security Solution**. Pulse **Avanzadas** y seleccione **Valores de seguridad de auditoría**. Ejecuta C:\Archivos de programa\IBM ThinkVantage\Common\WST\wst.exe para una instalación por omisión.

Los parámetros son:

Tabla 47.

Parámetros	Descripción
HardwarePasswords	Puede ser 1 ó 0, 1 mostrará esta sección, 0 la ocultará. Si no está presente, se muestra por omisión.
PowerOnPassword	Establece el valor de que se debe habilitar una contraseña de encendido, o el valor aparecerá con distintivos.
HardDrivePassword	Establece el valor de que se debe habilitar una contraseña de disco duro, o el valor aparecerá con distintivos.
AdministratorPassword	Establece el valor de que se debe habilitar una contraseña de administrador, o el valor aparecerá con distintivos.
WindowsUsersPasswords	Puede ser 1 ó 0, 1 mostrará esta sección, 0 la ocultará. Si no está presente, se muestra por omisión.
Password	Establece el valor de que se debe habilitar la contraseña de usuario o el valor aparecerá con distintivos.
PasswordAge	Establece el valor de cuál debe ser la antigüedad de la contraseña Windows en esta máquina, o el valor aparecerá con distintivos.
PasswordNeverExpires	Establece el valor de que la contraseña de Windows nunca caducará, o el valor aparecerá con distintivos.
WindowsPasswordPolicy	Puede ser 1 ó 0, 1 mostrará esta sección, 0 la ocultará. Si no está presente, se muestra por omisión.

Tabla 47. (continuación)

Parámetros	Descripción
MinimumPasswordLength	Establece el valor de cuál debe ser la longitud de la contraseña en esta máquina, o el valor aparecerá con distintivos.
MaximumPasswordAge	Establece el valor de cuál debe ser la antigüedad de la contraseña en esta máquina, o el valor aparecerá con distintivos.
ScreenSaver	Puede ser 1 ó 0, 1 mostrará esta sección, 0 la ocultará. Si no está presente, se muestra por omisión.
ScreenSaverPasswordSet	Establece el valor de que el protector de pantalla debe tener contraseña, o el valor aparecerá con distintivos.
ScreenSaverTimeout	Establece el valor de cuál debe ser el tiempo de espera excedido del protector de pantalla en esta máquina, o el valor aparecerá con distintivos.
FileSharing	Puede ser 1 ó 0, 1 mostrará esta sección, 0 la ocultará. Si no está presente, se muestra por omisión.
AuthorizedAccessOnly	Establece el valor de que se debe establecer el acceso autorizado para la compartición de archivos, o el valor aparecerá con distintivos.
ClientSecurity	Puede ser 1 ó 0, 1 mostrará esta sección, 0 la ocultará. Si no está presente, se muestra por omisión.
EmbeddedSecurityChip	Establece el valor de que se debe habilitar el chip de seguridad, o el valor aparecerá con distintivos.
ClientSecuritySolution	Establece el valor de qué versión de CSS debe estar en esta máquina, o el valor aparecerá con distintivos.

Otra opción para todos los valores es ignore, lo que significa que se muestra el valor, pero no se incluye este valor en la comparación. Mientras se ejecuta Security Advisor, un archivo HTML se graba en c:\ibmshare\wst.html y un archivo XML de datos sin formato se graba en c:\ibmshare\wst.xml

Ejemplo

A continuación se muestra una Sección [WST] que muestra todas las secciones y tiene todos los valores establecidos en sus valores por omisión:

```
[wst]
HardwarePasswords=1
PowerOnPassword=enabled
HardDrivePassword=enabled
AdministratorPassword=enabled

WindowsUsersPasswords=1
Password=enabled
PasswordAge=180
PasswordNeverExpires=false

WindowsPasswordPolicy=1
```

```
MinimumPasswordLength=6
MaximumPasswordAge=180

ScreenSaver=1
ScreenSaverPasswordSet=true
ScreenSaverTimeout=15

FileSharing=1
AuthorizedAccessOnly=true

ClientSecurity=1
EmbeddedSecurityChip=Enabled
ClientSecuritySolution=6.0.0.0
```

Para ocultar o mostrar Security Advisor, añada una sección en el archivo TVT.txt denominado WST. Existen varios valores que se pueden ocultar o personalizar, pero se deben añadir al archivo TVT.txt.

Si no desea utilizar Security Advisor y no desea que se muestre habilitado en la GUI, elimine el siguiente archivo ejecutable:

```
C:\Archivos de programa\IBM ThinkVantage\Common\WST\wst.exe
```

Asistente de transferencia de certificados

Si no desea utilizar el Asistente de transferencia de certificados y no desea que se muestre habilitado en la GUI, elimine el siguiente archivo ejecutable:

```
C:\Archivos de programa\IBM ThinkVantage\Client Security Solution
\certificatetransferwizard.exe
```

Asistente de Client Security

Este Asistente se utiliza para Tomar posesión del hardware, configurar el software y registrar usuarios. También se utiliza para generar scripts de despliegue mediante archivos XML. Se puede ejecutar el siguiente mandato para entender las funciones del asistente:

```
C:\Archivos de programa\IBM ThinkVantage\Client Security Solution\css_wizard.exe /?
```

Tabla 48.

Parámetro	Resultado
/h o /?	Visualiza el recuadro de mensaje de ayuda
/name:*NOMBREARCHIVO*	Precede a la vía de acceso calificada totalmente y al nombre de archivo del archivo de despliegue generado. El archivo tendrá una extensión .xml.
/encrypt	Cifra el archivo script utilizando cifrado AES. Si está cifrado, al nombre de archivo se añadirá la extensión .enc. Si no se utiliza el mandato /pass, se utiliza una frase de paso estática para ocultar el archivo.
/pass:	Precede a la frase de paso para la protección del archivo de despliegue cifrado.

Tabla 48. (continuación)

Parámetro	Resultado
/novalidate	Inhabilita las capacidades de comprobación de contraseña y frase de paso del asistente, de forma que se puede crear un archivo script en una máquina ya configurada. Por ejemplo, es posible que la contraseña de administrador en la máquina actual no sea la contraseña de administrador que se desee tener en toda la empresa. Utilice el mandato /novalidate para que pueda tener una contraseña de administrador distinta en la GUI de css_wizard durante la creación del archivo xml.

Aquí tiene un ejemplo de este mandato:

```
css_wizarde.exe /encrypt /pass:mi secreto /name:C:\DeployScript /novalidate
```

Nota: Si el sistema se está ejecutando en modalidad de emulación, el nombre del ejecutable es css_wizard.exe.

Herramienta de Cifrado/Descifrado del archivo de despliegue

Esta herramienta se utiliza para cifrar/descifrar los archivos de despliegue XML de Client Security. Se puede ejecutar el mandato siguiente para entender las funciones de la herramienta:

```
C:\Archivos de programa\IBM ThinkVantage\Client Security Solution\
xml_crypt_tool.exe. /?
```

Los parámetros se muestran en la Tabla 49:

Tabla 49.

Parámetros	Resultado
/h o /?	Visualiza el mensaje de ayuda
FILENAME	Nombre de vía de acceso y nombre de archivo totalmente calificados con la extensión .xml o .enc
encrypt o decrypt	Seleccione /encrypt para archivos .xml y /decrypt para archivos .enc.
PASSPHRASE	Parámetro opcional que es necesario si se utiliza una frase de paso para proteger el archivo.

Ejemplos:

```
xml_crypt_tool.exe "C:\DeployScript.xml" /encrypt "mi secreto"
```

y

```
xml_crypt_tool.exe "C:\DeployScript.xml.enc" /decrypt "mi secreto"
```

Herramienta de Proceso del archivo de despliegue

La herramienta vmserver.exe procesa los scripts de despliegue XML de Client Security. Se puede ejecutar el siguiente mandato para entender las funciones del asistente:

```
C:\Archivos de programa\IBM ThinkVantage\Client Security Solution\vmserver.exe /?
```

Tabla 50.

Parámetro	Resultado
FILENAME	El parámetro FILENAME debe tener una extensión de archivo xml or enc.
PASSPHRASE	El parámetro PASSPHRASE se utiliza para descifrar un archivo con la extensión enc.

Aquí tiene un ejemplo de este mandato:

```
Vmservere.exe  C:\DeployScript.xml.enc "mi secreto"
```

Nota: Si el sistema se está ejecutando en modalidad de emulación, el nombre del ejecutable es vmserver.exe

TPMENABLE.EXE

El archivo TPMENABLE.EXE se utiliza para activar o desactivar el chip de seguridad.

Tabla 51.

Parámetro	Descripción
/enable o /disable (Activa o desactiva el chip de seguridad)	Activa o desactiva el chip de seguridad.
/quiet	Oculta los indicadores de solicitud para la contraseña o los errores del BIOS.
sp:*contraseña*	Contraseña de supervisor/administrador del BIOS, no utilizar comillas alrededor de la contraseña.

Ejemplo de mandato:

```
tpmenable.exe /enable /quiet /sp:Mi ContBios
```

eGatherer

El mandato eGatherer se puede encontrar en C:\Archivos de programa\IBM ThinkVantage\common\egatherer\egather2.exe.

egathere2.exe crea una salida EG2 con la información recopilada. También puede crear un archivo de salida XML local que se almacena en la carpeta inicial. Tenga en cuenta que el archivo EG2 no es un formato interno.

Se crearán dos archivos XML, uno para la información del sistema y otro para la información demográfica. El nombre del archivo XML se crea combinando el fabricante, el tipo de modelo y el número de serie. Por ejemplo: IBM-2373Q1U-99MA4L7.XML, IBM-2373Q1U-99MA4L7.DEMOGRAPHICS.XML.

La exploración se puede ejecutar desde una línea de mandatos utilizando la siguiente sintaxis de la línea de mandatos:

egather2.exe [-help] [-batch] [-silent] [-nolimit] [-local] [-listprobes] [-probe probename *nombreprueba*]

- **-help**

  Muestra un mensaje corto de ayuda.
- **-batch**

No muestra la renuncia de responsabilidad.

- **-silent**

  No muestra nada durante la operación.
- **-nolimit**

  Recopila todo el registro de sucesos. El valor por omisión son las últimas 500 entradas.
- **-local**

  Crea un archivo XML local.
- **-listprobes**

  Lista las pruebas disponibles.
- **-probe**

  Lista las pruebas especificas.

MAPDRV

El mandato MAPDRV invocará la interfaz de usuario para correlacionar una unidad de red. El mandato MAPDRV.EXE se puede encontrar en el directorio C:\Archivos de programa\IBM ThinkVantage\Common\MND. La interfaz de la unidad de red correlacionada da soporte a los parámetros siguientes

Sintaxis:

```
mapdrv [conmutadores]
```

Si se especifica el mandato sin parámetros, se inicia la aplicación y la información se debe especificar manualmente.

Los códigos de retorno para todos los parámetros son:

- **0** = satisfactorio
- **> 0** = fallido

Tabla 52. Parámetros de MAPDRV

Parámetro	Resultado
/nodrive	Realiza la conexión de red sin asignar letra de unidad a la conexión.
/pwd	Contraseña de este usuario en esta compartición.
/set	Establece la compartición, el usuario y la contraseña utilizados por la Copia de seguridad y restauración.
/s	Silenciosa. No pregunta al usuario independientemente de si se realiza la conexión.
/timeout	Establece el valor de tiempo de espera excedido.
/unc	El nombre de compartición tiene el formato \\server\share
/user	Nombre de usuario para esta compartición.

Cuando se utiliza el mandato /SET, se añadirá la siguiente sección al archivo TVT.TXT. Esto se muestra en el ejemplo siguiente donde se utilizan los parámetros /UNC/USER y PWD:

```
mapdrv /set /unc nombrecompartición /user nombreusuario /pwd contraseña
[mapdrv]
UNC=\\test\test
User=1EE22597AE4D
PWD=04E22197B34D95943ED5A169A0407C5C
```

Control del Gestor de arranque de Rescue and Recovery (BMGR32)

La interfaz de la línea de mandatos de la interfaz del gestor de arranque es BMGR32. Está ubicada en el directorio C:\Archivos de programa\IBM ThinkVantage\Common\BMGR. La tabla siguiente presenta los conmutadores y sus resultados para BMGR32.

Tabla 53. Parámetros de BMGR32

bmgr32	**Resultado**
/B0	Arranca en la partición 0 (en base al orden de la tabla de particiones).
/B1	Arranca en la partición 1.
/B2	Arranca en la partición 2.
/B3	Arranca en la partición 3.
/BS	Arranca en la Partición de servicio.
/BW	Arranca en la partición protegida de Rescue and Recovery.
/BWIN	Restablece la petición para arrancar en WINPE. Se debe llamar a este parámetro antes del arranque.
/CFG*archivo*	Aplica los parámetros del archivo de configuración. Consulte “Interfaz de la línea de mandatos RRCMD” en la página 174 para ver detalles acerca del archivo de configuración.
/DS	Vuelve al sector de datos de MBR (basado en 0).
/D*n*	Aplica los cambios al disco n, donde n está basado en 0, (valor por omisión: disco que contiene la variable de entorno ″SystemDrive″ o ″C:\″ si ″SystemDrive″ no está definida).
/H0	Oculta la partición 0.
/H1	Oculta la partición 1.
/H2	Oculta la partición 2.
/H3	Oculta la partición 3.
/HS	Oculta la Partición de servicio.
/P12	Oculta la Partición de servicio estableciendo el tipo de configuración en 12.
/INFO	Visualiza la información de la unidad de disco duro (comprueba si hay 8 sectores libres).
/INFOP	Visualiza la información de la unidad de disco duro (comprueba si hay 16 sectores libres).
/M0	El entorno de Rescue and Recovery está ubicado en la Partición de servicio.
/M1	El entorno Rescue and Recovery está ubicado en C:\PARTITION (arranque dual en Windows y Windows PE).
/M2	El entorno de Rescue and Recovery está ubicado en la Partición de servicio con DOS (arranque dual en Windows PE y DOS; sólo en sistemas de Lenovo o IBM).

Tabla 53. Parámetros de BMGR32 (continuación)

bmgr32	Resultado
/OEM	El sistema no es un sistema de IBM o Lenovo. Esto fuerza una segunda comprobación pulsando la tecla F11 (valor por omisión) después de la POST. Es posible que esto sea necesario en sistemas antiguos de IBM. Éste es también el valor por omisión para la versión de OEM de Rescue and Recovery.
/Patch*n*	Utilizado sólo para que el programa de instalación establezca una variable a la que pueda acceder el programa de parche de MBR.
Patchfile*nombrearchivo*	Utilizado sólo para que el programa de instalación instale un parche de MBR.
/PRTC	Utilizado sólo para que el programa de instalación recupere el código de retorno del parche.
/IBM	El sistema es un sistema de IBM o Lenovo.
/Q	Silenciosa
/V	Detallada
/R	Rearranca el sistema.
/REFRESH	Restablece las entradas de la tabla de particiones en el sector de datos.
/TOC *valortablacontenido*	Establece la ubicación de la tabla de contenido del BIOS (16 caracteres que representan 8 bytes de datos).
/U0	Muestra la partición 0.
/U1	Muestra la partición 1.
/U2	Muestra la partición 2.
/U3	Muestra la partición 3.
/US	Muestra la partición de servicio.
/F*mbr*	Carga el programa de registro de arranque maestro de RRE.
/U	Descarga el programa de registro de arranque maestro de RRE.
/UF	Fuerza la instalación o desinstalación del programa MBR.
/?	Lista las opciones de la línea de mandatos.

Cuando se llama a bmgr.exe con un atributo /info, se vuelca la siguiente información:

- **MBR adicional**

  Números de sector que contienen el MBR, distintos del primer sector.
- **Datos**

  Número de sector del sector de datos utilizados por el MBR.
- **Índices de parche**

  Números de sectores de los parches que se hayan aplicado utilizando el MBR.
- **Retorno de suma de comprobación**

  Debe ser 0 si no hay errores de suma de comprobación.
- **Partición de arranque**

  Índice de la tabla de particiones basado en 1 de la Partición de servicio.
- **Partición Alt**

Índice de la tabla de particiones que apunta al área arrancable de DOS, si existe una.

- **MBR original**

  Número de sector donde se almacena el MBR original de la máquina.
- Distintivo de **IBM**

  Valor del sector de datos (1 si se trata de un sistema de IBM o Lenovo, 0 si no)
- **Configuración de arranque**

  Describe la opción de instalación utilizada para describir el diseño de la máquina. Si se ha utilizado una partición de servicio o una partición virtual.
- **Firma**

  Valor de firma que se encuentra en el sector de datos y el primer sector, debe contener "NP"
- **Duración de pausa**

  Es el número de segundos de ¼ que se debe esperar si se visualiza en mensaje de F11 en la pantalla.
- **Código de exploración**

  Qué clave se utiliza al arrancar en el Área de servicio. 85 es para la tecla F11.
- **RR**

  BMGR no lo utiliza, pero lo establece Rescue and Recovery.
- **Partición activa ant**

  Cuando se arranca en el Área de servicio, este valor contiene el índice de la tabla de particiones de la partición activa anteriormente.
- **Estado de arranque**

  Lo utiliza MBR para determinar el estado actual de la Máquina. 0 – Arranque normal en el sistema operativo, 1 – Arranque en el sistema operativo de servicio, 2 – Arranque de nuevo en el sistema operativo normal desde el sistema operativo de servicio.
- **Distintivo de arranque alternativo**

  Arranque en el sistema operativo alternativo, DOS por ejemplo
- **Tipo de partición anterior**

  Cuando se arranca en el Área de servicio, este valor contiene el tipo de partición en el que se estableció la Partición de servicio antes de arrancar en ella.
- **Índice MBR anterior de IBM**

  Utilizado por el instalador.
- **Parche IN: OUT**

  Los valores de entrada y salida del código de parche, si se utiliza.
- **Mensaje de F11**

  Mensaje que mostrará al usuario si no están soportadas las llamadas al BIOS adecuadas

RELOADSCHED

Este mandato vuelve a cargar los valores planificados que están definidos en TVT.TXT. Si realiza cambios en TVT.TXT para la planificación, debe realizar este mandato para activar los cambios.

Ejemplo de mandato:

```
C:\Archivos de programa\IBM ThinkVantage\Rescue and Recovery\reloadsched
```

Interfaz de la línea de mandatos RRCMD

La interfaz primaria de la línea de mandatos de Rescue and Recovery es RRCMD. Este mandato está ubicado en el subdirectorio C:\Archivos de programa\IBM ThinkVantage\Rescue and Recovery\reloadsched.exe. Consulte la siguiente información para utilizar la interfaz de la línea de mandatos para Rescue and Recovery.

Sintaxis:

`RRcmd` *`mandato filter=filterfile ubicación=c`* `[name=`*`abc`*` | level=`*`x`*`] [silent]`

Tabla 54. Parámetros de RRcmd

Mandato	Resultado
`Backup`	Inicializa una operación de copia de seguridad normal (debe incluir los parámetros de nombre y ubicación).
`Restore`	Inicializa una operación de restauración normal (debe incluir ubicación y nivel).
`List`	Lista archivos que se incluyen en el nivel de copia de seguridad (debe incluir la ubicación y el nivel).
`Basebackup`	Inicializa una copia de seguridad base alternativa. No se utiliza como una base para las copias de seguridad incrementales, y debe incluir la ubicación, el nombre y el nivel. El nivel debe ser menor que 99. Si ya existe otra copia de seguridad base con el mismo nivel, se sobregrabará.
`Sysprepbackup`	Realiza una operación de copia de seguridad en el Área previa al escritorio después de que se rearranque el sistema. La utilización primaria de esta característica es capturar una copia de seguridad de Sysprep. **Notas:** 1. En algunos casos, la barra de progreso no se moverá. Si esto sucede, puede verificar si se está realizando la copia de seguridad escuchado el sonido de la unidad de disco duro. Cuando se complete la copia de seguridad, recibirá un mensaje indicándole que la copia de seguridad se ha completado. 2. Si está estableciendo una contraseña al crear una copia de seguridad de Sysprep en la red, el archivo de contraseña no se grabará en la ubicación de la copia de seguridad hasta que se haya realizado una copia de seguridad incremental. Aquí se muestran dos soluciones alternativas: a. Cree una copia de seguridad local de Sysprep y copie las copias de seguridad en la red o en la unidad USB. b. Cree una copia de seguridad incremental en la red o en la unidad USB después de la copia de seguridad de Sysprep y guarde o borre la copia de seguridad incremental.
`Copy`	Copia las copias de seguridad de una ubicación a otra. También se denomina archivado, y debe incluir la ubicación.
`Rejuvenate`	Rejuvenece el sistema operativo en la copia de seguridad especificada.
`Delete`	Suprime las copias de seguridad. Debe incluir la ubicación.

Tabla 54. Parámetros de RRcmd (continuación)

Mandato	Resultado
`Changebase`	Cambia los archivos de todas las copias de seguridad en base al contenido del archivo file.txt. Las opciones del file.txt son: **A** Añadir **D** Suprimir **RS** Sustituir
`migrate`	Crea archivo de migración a partir de una copia de seguridad.
`filter=`*`nombrefiltro`*	Identifica los archivos y las carpetas que se restaurarán y no modifica otros archivos. Se utiliza solamente con el mandato **restore**.
`Location=`*`c`*	Se puede seleccionar uno o varios de los siguientes con el resultado asociado. **L** Para la unidad de disco duro local primaria **U** Para la unidad de disco duro USB **S** Para la segunda unidad de disco duro **N** Para la red **C** Para restaurar desde CD/DVD
`name=`*`abc`*	Donde *abc* es el nombre de la copia de seguridad.
`level=`*`x`*	Donde *x* es un número de 0 (para la base) al número máximo de copias de seguridad incrementales (sólo utilizado con la opción de restauración). Para los mandatos de copia de seguridad, el mandato level=*x* sólo es necesario si se realiza una copia de seguridad de administrador (igual a o mayor que 100, por ejemplo). **Notas:** 1. Para restaurar a partir de la última copia de seguridad, no proporcione este parámetro. 2. Todas las características de copia de seguridad y restauración se direccionan a través del servicio, de forma que se mantenga el secuenciado adecuado, se realicen las devoluciones de llamada, por ejemplo. El mandato backup se sustituye con las opciones de la línea de mandatos.)

Formato del archivo de configuración del Gestor de arranque	El formato del archivo de configuración del gestor de arranque es compatible con la versión anterior del gestor de arranque. Cualquier conmutador que no aparezca a continuación está soportado. El formato de archivo es un archivo de texto donde cada entrada está en una lista separada.
	
	`<PROMPT1=es el texto`
	`que aparecerá en el indicador de solicitud de F11>`
	`<KEY1=F11>`
	`<WAIT=40>`

System Migration Assistant

El módulo es un programa de la línea de mandatos compatible con el archivo SMABAT.EXE antiguo de SMA4.2. Los parámetros del mandato y la tarjeta de control (Commands.TXT) al módulo deben ser compatibles con SMA 4.2.

Active Update

Active Update es una tecnología de eSupport que utiliza los clientes de actualización en los sistemas locales para entregar los paquetes que se deseen de la Web sin ninguna interacción del usuario. Active Update consulta qué clientes de actualización están disponibles y utiliza el cliente de actualización disponible para instalar el paquete que se desee. Active Update iniciará ThinkVantage System Update o Software Installer en el sistema.

Para determinar si Active Update Launcher está instalado, compruebe la existencia de la siguiente clave de registro: HKLM\Software\Thinkvantage\ActiveUpdate.

Para determinar si Active Update Launcher está configurado para permitir Active Update, HKLM\Software\IBMThinkvantage\Rescue and Recovery debe comprobar en su propia clave de registro el valor del atributo EnableActiveUpdate. EnableActiveUpdate=1 establecerá el elemento de menú Active Update debajo del menú de Ayuda.

Active Update

Para determinar si Active Update Launcher está instalado, compruebe si existe la siguiente clave de registro:

```
HKLM\Software\TVT\ActiveUpdate
```

Para determinar si el archivo TVT.TXT está configurado para permitir Active Update, TVT debe comprobar en su propia clave de registro el valor del atributo EnableActiveUpdate. Si EnableActiveUpdate=1, TVT debe añadir el elemento de menú Active Update debajo del menú de Ayuda.

Para llamar a Active Update, el TVT que realiza la llamada debe iniciar el programa Active Update Launcher y pasar el archivo de parámetros (consulte Archivo de parámetros de Active Update para ver una descripción del archivo de parámetros).

Utilice los pasos siguientes para invocar a Active Update:

1. Abra la clave de registro de Active Update Launcher:

   ```
   HKLM\Software\TVT\ActiveUpdate
   ```

2. Obtenga el valor del atributo Path.
3. Obtenga el valor del atributo Program.
4. Concadene los valores encontrados en los atributos Path y Program para formar la serie del mandato.
5. Añada el archivo de parámetros (consulte Archivo de parámetros de Active Update) a la serie del mandato.
6. Ejecute la serie del mandato. Aquí tiene un ejemplo del aspecto que puede tener la serie del mandato resultante:

   ```
   C:\Archivos de programa\ThinkVantage\ActiveUpdate\activeupdate.exe C:\Program
    Files\ThinkVantage\RnR\tvtparms.xml
   ```

La forma recomendada de invocar a Active Update es de forma asíncrona, de forma que no se bloquee el TVT que realiza la llamada. Si es necesario terminar el TVT que realiza la llamada antes de instalar la actualización, es responsabilidad del programa de instalación de la actualización terminar el TVT.

Archivo de parámetros de Active Update

El archivo de parámetros de Active Update contiene los valores que se deben pasar a Active Update. Actualmente, sólo TargetApp (el nombre de TVT) se pasa, como se muestra en este ejemplo:

```
<root>
       <TargetApp>ACCESSIBM</TargetApp>
</root>
```

```
<root>
       <TargetApp>1EA5A8D5-7E33-11D2-B802-00104B21678D</TargetApp>
</root>
```

Apéndice D. Herramientas del administrador

Las tecnologías ThinkVantage proporcionan herramientas que pueden invocar los administrador de TI de la empresa.

Antidote Wizard

Para obtener información acerca de Antidote Wizard, consulte el Apéndice F, "Consulta de mandatos y ejemplos de Antidote Delivery Manager", en la página 185.

BMGR CLEAN

CleanMBR borra el Registro de arranque maestro. Este programa se puede utilizar cuando se encuentre con un fallo de la instalación de Rescue and Recovery, como por ejemplo no poder instalar Rescue and Recovery con menos de los sectores libres necesarios para que se instale el gestor de arranque.

Notas:

1. Después de ejecutar esta herramienta, las aplicaciones que están utilizando MBR quedan inutilizables. Por ejemplo, SafeGuard Easy, SafeBoot y la versión de MBR de Computrace etc.
2. La herramienta se debe ejecutar antes de instalar Rescue and Recovery.
3. Utilice cleanmbr.exe para DOS y CleanMBR32.exe se puede utilizar en Windows.
4. Después de ejecutar CleanMBR de DOS, ejecute FDISK /MBR; se pondrá en MBR.

Los parámetros para CleanMBR32.exe son los siguientes:

Tabla 55.

Parámetro (necesario):	**Descripción**
/A	Borra MBR e instala PC DOS MBR
Parámetro (Opcional):	
/Dn	Aplica los cambios a la unidad. Utilice *n*=0 para la primera unidad.
/Y	Sí para todos
/?	Visualiza la ayuda
/H	Visualiza la ayuda

CLEANDRV.EXE

Borra todos los archivos de la unidad. Después de ejecutar este mandato no habrá ningún sistema operativo. Consulte "Instalación de Rescue and Recovery en una partición de servicio de tipo 12" en la página 135 para obtener más información.

CONVDATE

El programa de utilidad Convdate se proporciona como parte de las herramientas de administración de Rescue and Recovery. Este programa de utilidad se utiliza para determinar los valores hexadecimales de la fecha y la hora y para convertir los valores de la fecha y la hora en valores hexadecimales y que se puedan utilizar para establecer una fecha y hora personalizadas en el campo Backup de TVT.TXT

```
[Backup0]
StartTimeLow=0xD5D53A20
StartTimeHigh=0x01C51F46
```

Para ejecutar el programa de utilidad, haga lo siguiente:

1. Extraiga las herramientas de administración de Rescue and Recovery desde http://www.lenovo.com/thinkvantage
2. Abra una ventana de la línea de mandatos
3. Escriba Convdate

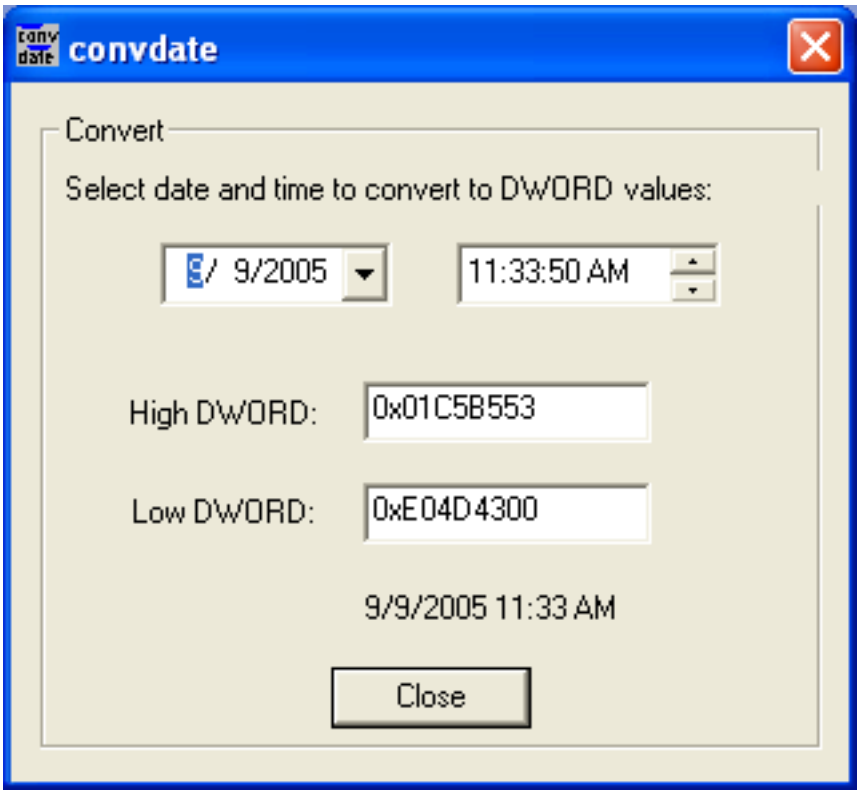

Figura 5. Ventana convdate

4. Escriba la fecha y la hora en los campos debajo de Select date and time (Seleccionar fecha y hora) para convertir los valores DWORD.
5. Los valores correspondientes del archivo TVT..TXT son los siguientes:
   - High DWORD=StartTimeHigh
   - Low Dword=StartTimeLow

CREAT SP

Este mandato crea una partición para la partición de servicio con los megabytes que se deseen. La letra de la unidad es opcional.

La sintaxis es:

```
createsp size=x drive=x /y
```

Los parámetros para CREAT SP son:

Tabla 56.

Parámetros	Descripción
size=*x*	Tamaño de la partición de servicio que se va a crear, en Megabytes.
drive=*x*	Número de la unidad donde se va a crear la partición de servicio. Si no se especifica, se utilizará la primera unidad que no sea USB. Este parámetro es opcional.
/y	Suprime la confirmación de que se está borrando la unidad. Este parámetro es opcional.

Nota: bmgr32.exe debe estar en el mismo directorio que createsp.exe y se debe ejecutar desde WinPE.

RRUTIL.EXE

Para obtener información acerca de RRUTIL.EXE, consulte el “Área previa al escritorio” en la página 22.

SP.PQI

Este archivo se puede utilizar para crear una partición de servicio de tipo 12. Consulte “Instalación de Rescue and Recovery en una partición de servicio de tipo 12” en la página 135 para obtener más información.

Apéndice E. Tareas de usuario

Es posible que los usuarios no puedan realizar ciertas tareas, en base a los derechos de usuario. Las tablas siguientes resumen la capacidad de las tareas básicas con los permisos de ID de usuario del sistema operativo por omisión Usuario/Usuario con limitaciones, Usuario avanzado y Administrador. Las tareas y las capacidades difieren según el sistema operativo Windows.

Windows XP

La tabla siguiente presenta las tareas que los usuarios con limitaciones, avanzados y administrativos pueden realizar en Rescue and Recovery en un entorno Windows XP.

Tabla 57. Tareas de usuario de Windows XP

Los usuarios de Windows XP pueden realizar lo siguiente:	**Usuario con limitaciones**	**Usuario avanzado**	**Administrador**
Crear ISO de soporte de rescate	No	No	Sí (con la línea de mandatos proporcionada a continuación)
Crear soporte de CD arrancable	Sí	Sí	Sí
Crear soporte arrancable en unidad de disco duro USB	No	No	Sí
Inicializar copia de seguridad	Sí	Sí	Sí
Inicializar restauración en el entorno de Rescue and Recovery (RRE - Rescue and Recovery Environment)	Sí	Sí	Sí
Realizar la restauración de un único archivo en RRE	No (Windows) Sí (Área de arranque de Windows)	No (Windows) Sí (Área de arranque de Windows)	Sí
Establecer inclusión y exclusión en la interfaz de Rescue and Recovery	Sí	Sí	Sí
Realizar copia de seguridad en una unidad de red	Sí	Sí	Sí
Planificar copias de seguridad	Sí	Sí	Sí

Windows 2000

La tabla siguiente presenta las tareas que los usuarios con limitaciones, avanzados y administrativos pueden realizar en Rescue and Recovery en un entorno Windows 2000.

Tabla 58. Tareas de usuario de Windows 2000

Los usuarios de Windows 2000 pueden realizar lo siguiente:	**Usuario con limitaciones**	**Usuario avanzado**	**Administrador**
Crear ISO de soporte de rescate	No	No	Sí (con la línea de mandatos proporcionada a continuación)
Crear soporte de CD arrancable	Sí	Sí	Sí
Crear soporte arrancable en unidad de disco duro USB	No	No	Sí
Inicializar copia de seguridad	Sí	Sí	Sí
Inicializar restauración en el entorno de Rescue and Recovery (RRE - Rescue and Recovery Environment)	Sí	Sí	Sí
Realizar la restauración de un único archivo en RRE	No (Windows) Sí (Área de arranque de Windows)	No	Sí
Establecer inclusión y exclusión en la interfaz de Rescue and Recovery	Sí	Sí	Sí
Realizar copia de seguridad en una unidad de red	No	No	Sí
Planificar copias de seguridad	Sí	Sí	Sí

Crear soporte de rescate

Los administradores pueden utilizar las líneas de mandatos siguientes para crear la ISO del soporte de rescate. Estas líneas de mandatos le permitirán crear el archivo ISO necesario y éste se colocará automáticamente en el directorio C:\Archivos de programa\IBM ThinkVantage\Rescue and Recovery\rrcd\:

```
:: Esta línea creará la ISO de forma silenciosa y no lo grabará

C:\Archivos de programa\IBM ThinkVantage\Common\Python24\python" "C:\Archivos de
programa\IBM ThinkVantage\Common\spi\mkspiim.pyc /scripted


 /scripted

:: Esta línea creará la ISO con la interacción del usuario y no lo grabará

C:\Archivos de programa\IBM ThinkVantage\Common\Python24\python C:\Archivos de
programa\IBM ThinkVantage\Common\spi\mkspiim.pyc /noburn

 /noburn
```

Apéndice F. Consulta de mandatos y ejemplos de Antidote Delivery Manager

Se proporciona una herramienta de empaquetado de la línea de mandatos para que el administrador cree mensajes. Además, Antidote Delivery Manager proporciona funciones especiales de mandatos para utilizar en los mensajes.

Guía de mandatos de Antidote Delivery Manager

La interfaz de la línea de mandatos de la interfaz del gestor de arranque es BMGR32. Está ubicado en el directorio C:\Archivos de programa\IBM ThinkVantage\Rescue y Recovery\ADM. La tabla siguiente presenta los conmutadores y sus resultados para BMGR32.

Tabla 59. Mandatos de Antidote Delivery Manager

Mandatos	Descripción
APKGMES [/KEY *archivoClaves*|/NEWKEY *archivoClaves*|/NOSIG] *directorio_mensajes nombre_mensaje*	Para APKGMES /KEY se creará un archivo de mensaje a partir del contenido del *TVT.TXTdirectorio_mensajes*. El directorio debe contener un archivo denominado GO.RRS. Si se utiliza el parámetro /KEY, se recuperará una clave de firma de keyfile.prv y la clave en keyfile.pub se debe distribuir a todos los clientes que procesarán el mensaje. Por omisión, se utilizará el archivo de claves "KEYFILE.PRV". El parámetro /NEWKEY se puede utilizar para crear una clave. Si no se desea la firma, si especifica /NOSIG evitará la firma. Se añadirá una indicación de fecha al final del nombre del mensaje, como por ejemplo *nombre_mensaje*AAMMDDHHmm.zap.
REBOOT [/*RR*|/Win] [/wait | /f]	Este mandato reinicia la máquina. Sin parámetros, rearranca con la secuencia de arranque normal. El parámetro RR significa rearrancar en Rescue and Recovery y WIN significa rearrancar en el sistema operativo normal. El rearranque no se producirá hasta que se salga del script, así que éste debería ser el último mandato en un script. El mandato opcional WAIT fuerza al sistema a rearrancar en el entorno especificado en el siguiente rearranque (manual o causado por otro mecanismo). El parámetro /f fuerza al sistema a rearrancar ahora y no permite al usuario guardar información de las aplicaciones abiertas. Si no se especifica ningún parámetro, el programa adopta el valor por omisión de /win (no se especifican /wait y /f).

Tabla 59. Mandatos de Antidote Delivery Manager (continuación)

Mandatos	Descripción
`RETRYONERROR [ON|OFF] reintentos`	Por omisión, sólo se puede intentar un script una vez. Sin embargo, si es importante continuar intentando un script hasta que funcione, se puede utilizar el mandato RETRYONERROR para notificar a la función de buzón de correo que siga intentando ejecutar dicho script un número finito de veces, tal y como se especifique en el parámetro de reintentos. Si no se ha especificado ningún número, el valor por omisión es 3. Se puede establecer un valor por omisión global en el archivo TVT.TXT en la sección de rescate `retries = reintentos`. También se puede establecer el parámetro de reintentos en FOREVER, lo que causaría que se produjera un bucle infinito.
`MSGBOX /msg texto del mensaje [/head texto_cabecera] [/OK] [/CANCEL]| [/TIMER tiempo_espera_excedido] /B3`	El mandato MSGBOX visualizará un mensaje al usuario final, si éste ha iniciado sesión. El mensaje permanecerá en pantalla y el script se bloqueará hasta que se exceda el tiempo de espera, se pulse el botón Cancelar o se presione el botón **Aceptar** (si se ha especificado /OK). En el panel no habrá ningún botón Cancelar si no se ha especificado /CANCEL, y no será fácil deshacerse de la pantalla. El mandato devolverá lo siguiente: • 0 = Se ha pulsado Aceptar • 1 = CANCELAR • 2 = El temporizador ha caducado El texto del mensaje se puede formatear utilizando \n y \t para representar nueva línea y tabulador, respectivamente.
`NETWK [/D|/E|/A [/IP dirección_ip | /DN nombre_dominio] [/NM máscara_red]`	NETWK /D (inhabilitar) detendrá todo el tráfico de red inhabilitando todos los adaptadores de red. Las comunicaciones de red se inhabilitarán hasta que se ejecute el mandato NETWK /E (habilitar). NETWK /A restringe las comunicaciones de red a la dirección IP especificada por el conmutador /IP (decimal separado por puntos) o /DN (nombre de DN). El conmutador /NM proporciona la máscara de red. Si no se proporciona /NM, sólo será accesible la única máquina especificada por /IP o /DN. El estado de este mandato persiste después del rearranque, así que las comunicaciones de red se deben habilitar explícitamente.
`APUBKEY [/ADD|/DELETE] clave_pública_codificada_asn_1`	Un mandato APASSWD permite a un administrador gestionar de forma remota las claves de firma de mensaje de Antidote Delivery Manager en cada PC. Se almacena más de una clave en cada PC. Si se procesa un mensaje firmado, se probará cada clave hasta que se encuentre una clave satisfactoria. Las claves no reciben nombres individuales, así que se debe hacer referencia a ellas por el contenido. Se puede añadir una nueva clave utilizando el parámetro ADD y se puede suprimir con el parámetro DELETE. Tenga en cuenta que si hay claves especificadas en TVT.TXT, los mensajes no firmados (aquellos creados con /NOSIG) ya no se podrán utilizar.

Tabla 59. Mandatos de Antidote Delivery Manager (continuación)

Mandatos	Descripción
AUNCPW [/Add|/CHANGE|/DELETE] *unc* [/USER *idusuario*] [/PWD *contraseña*] [/REF *nombre_ref*]	Este mandato le permite añadir, cambiar o suprimir una contraseña para una unidad de red. El nombre de referencia se puede utilizar como un atajo en un mensaje en lugar de utilizar el UNC. Los valores de retorno son: • 0 = satisfactorio • 1 = no se puede establecer la información proporcionada • 2 = satisfactorio, pero ya se ha definido un UNC distinto que tiene el mismo nombre de referencia.

Tabla 59. Mandatos de Antidote Delivery Manager (continuación)

Mandatos	Descripción
`XMLtool para condicionales`	Condicionales (eGatherer, información del hardware actual) • **Uso:** xmltool.exe *nombrearchivo víaaccesox función elemento_comparación valor* donde: – **nombrearchivo** Vía de acceso y nombre del archivo del archivo XML – **víaaccesox** Vía de acceso x calificada totalmente del valor – **función** Debe ser uno de los siguientes valores: - /C, compara los valores (se debe proporcionar también el elemento de comparación y el valor) - /F , pone el valor especificado en %IBMSHARE%\RET.TXT – **Elemento de comparación:** Debe ser uno de los siguientes: - LSS - LEQ - EQU - GTR - GEQ - NEW – **Valor:** La entrada XML se compara con este valor. • Valores de retorno: – **0** La comparación se evalúa como verdadera (/c) – **1** La comparación se evalúa como falsa – **2** Parámetros incorrectos de la línea de mandatos – **3** Error al abrir el archivo XML (no está presente o el archivo tiene errores) – **4** El XPATH especificado no ha devuelto ningún valor • **Ejemplo:** `xmltool.exe %ibmshare%\\ibmegath.xml //system_summary/bios_version GEQ 1UET36WW`

Tabla 59. Mandatos de Antidote Delivery Manager (continuación)

Mandatos	Descripción
INRR	El mandato INRR se puede utilizar para determinar si el script se está ejecutando en el entorno de Rescue and Recovery. Los valores de retorno son: • 0 = el sistema operativo actual es PE • 1 = el sistema operativo actual no es PE • >1 = Error
STATUS [/QUERY *ubicación nombre_mensaje* | /CLEAR *ubicación]*	El mandato STATUS /QUERY se puede utilizar para determinar si se ha ejecutado un script o si está en cola para ser ejecutado. El valor de la ubicación debe ser el siguiente: • **FAIL** El mensaje ya se ha ejecutado y ha fallado. • **SUCCESS** El mensaje se ha completado satisfactoriamente. • **WORK** El mensaje se está ejecutando actualmente o se ejecutará la próxima vez que se ejecute Antidote Delivery Manager. • **CACHE** El mensaje está en cola para ser ejecutado. El mandato STATUS/CLEAR borrará la *ubicación* especificada. Los valores de retorno son: • 0 = si se ha encontrado el mensaje especificado o el mandato se ha completado satisfactoriamente • 1 = si el mensaje especificado no se ha encontrado o si el mandato ha fallado

Mandatos de Microsoft soportados

Tabla 60. Mandatos de Microsoft soportados

Mandatos	Descripción
ATTRIB.EXE	Visualiza o cambia los atributos del archivo
CACLS.EXE	Visualiza o modifica las listas de control de acceso (las ACL) de los archivos
CHKDSK.EXE	Comprueba un disco y visualiza un informe de estado
COMP.EXE	Compara el contenido de dos archivos o de dos conjuntos de archivos
COMPACT.EXE	Visualiza o modifica la compresión de archivos en particiones NTFS
CONVERT.EXE	Convierte volúmenes FAT a NTFS. No se puede convertir la unidad actual
DISKPART.EXE	Particiona una unidad
FC.EXE	Compara dos archivos o dos conjuntos de archivos y visualiza las diferencias entre ellos
FIND.EXE	Busca una serie de caracteres de texto en un archivo o en varios archivos

Tabla 60. Mandatos de Microsoft soportados (continuación)

Mandatos	Descripción
FINDSTR.EXE	Busca cadenas de caracteres en archivos.
FORMAT.COM	Formatea un disco para utilizarlo con Windows.
LABEL.EXE	Crea cambios o suprime la etiqueta de volumen de un disco.
NET.EXE	Proporciona los mandatos de las comunicaciones de red.
PING.EXE	Comprueba si se puede conectar con un recurso de red.
RECOVER.EXE	Recupera información legible de un disco erróneo o defectuoso.
REG.EXE	Manipulación del registro
REPLACE.EXE	Sustituye archivo.
RRCMD.EXE	Ejecuta Copias de seguridad desde el sistema operativo o restaura desde el sistema operativo o la entrada de clasificaciones de RR.
SORT.EXE	Clasifica entradas.
SUBST.EXE	Asocia una vía de acceso a una letra de unidad.
XCOPY.EXE	Copia archivos y árboles de directorios.

Preparación e instalación

Preparación

Si se utilizará una clave de firma, el administrador necesita ejecutar la herramienta de empaquetado con el parámetro /NEWKEY para generar una nueva clave de firma.

Configuración

Serán necesarios varios elementos de configuración. Los elementos aparecen en el archivo TVT.TXT:

Depósito

Cada cliente necesita lista de depósitos. Ésta debe incluir disquete y C:\, así como una unidad de red como mínimo especificada con un UNC; `mailbox =` que es la unidad y la vía de acceso a las ubicaciones del buzón de correo, con una coma, y separadas en orden de importancia. Ejemplo:

```
[rescue] mailbox = %y%\antidote, c:\antidote
```

Información de planificación

La Modalidad de planificación es la frecuencia de comprobaciones.

Tabla 61. Modalidades de comprobación

Modalidad de comprobación	
SCHED_NONE	0x000
SCHED_MINUTELY	0x001
SCHED_DAILY	0x002
SCHED_WEEKLY	0x004
SCHED_MONTHLY	0x008

Tabla 61. Modalidades de comprobación (continuación)

Modalidad de comprobación	
SCHED_STARTUP	0x010
SCHED_WAKEUP	0x020
SCHED_USB_ATTACH	0x040
SCHED_NETWORK_ATTACH	0x080

```
[Scheduler]
Task1=rescuerecovery
Task2=Rescue

[rescue]
ScheduleFrequency=0
ScheduleMode=0x02
TaskShow=1
Task=c:\Archivos de programa\IBM ThinkVantage\Rescue and Recovery\adm\mailman.exe
ScheduleHour=11
ScheduleMinute=28
ScheduleDayOfTheWeek=3
ScheduleWakeForBackup=0
```

Clave de firma

Si se utilizan claves de firma, éstas se deben distribuir al cliente. El archivo keyfile.pub creado por el mandato APKGMES contiene la clave. Cada clave de firma pública autorizada aparece en el archivo TVT.TXT como: `pubkey`*`X`* `= ...` donde *X* se sustituye por un entero, y se pueden almacenar hasta 9 claves públicas. Utilice la función APUBKEY para establecer este valor `nosig =`. Si está establecido en 1, permitirá que se ejecuten los paquetes sin firma (paquetes creados con el parámetro /NOSIG).

Nota: Si no está establecido en 1, o si las claves públicas están presentes en el archivo TVT.TXT, los paquetes sin firma no se ejecutarán.

Unidades de red

Los valores siguientes se establecen utilizando la función AUNCPW `RscDrvY`. Cada sección `RscDrv` contiene información sobre una compartición de red. Se pueden definir hasta 10 comparticiones de red para Antidote Delivery Manager.

- UNC = UNC de la unidad a la que necesita que se conecte Antidote Delivery Manager.
- User = Nombre de usuario cifrado
- Pwd = Nombre de contraseña cifrada
- Ref = Nombre de referencia que se asociará con esta conexión

Instalación en clientes

Rescue and Recovery 2.0 se debe instalar en todos los clientes. La configuración preparada anteriormente se puede incluir en la instalación o bien realizarla posteriormente.

Infraestructura del servidor

El administrador debe establecer comparticiones de red para el depósito o proporcionar un sitio FTP o HTTP. Es posible que sea necesario un depósito adicional para arreglos y parches.

Prueba simple del sistema – Visualizar notificación

Preparación y empaquetado de scripts

Grabe un script GO.RRS en cualquier máquina donde se haya instalado Antidote Delivery Manager. Incluya una línea `MSGBOX /MSG "Hola gente" /OK`. Ejecute el mandato directamente desde el indicador de la línea de mandatos para asegurarse de que funciona de la forma deseada. A continuación, ejecute el mandato APKGMSG en el directorio que contiene GO.RRS para crear un mensaje. Coloque el archivo de mensaje en uno de los directorios del depósito de la máquina y vigile que funciona correctamente.

Despliegue

Antes de desplegar Antidote Delivery Manager, debe realizar estos pasos:

1. Determine las ubicaciones de los buzones de correo:
   - Los *buzones de correo* están definidos como directorios en las comparticiones de red, la unidad de disco duro o un soporte extraíble de un sistema local o un sitio FTP o HTTP.
   - Es posible que encuentre útil disponer de varios buzones de correo en caso de que uno de ellos no esté accesible. Puede definir hasta diez ubicaciones de buzón de correo.
   - Los buzones de correo basados en la red deben ser de sólo lectura para los clientes y el acceso de grabación debe estar restringido.
2. Configure los buzones de correo en el archivo TVT.TXT:
   - En un sistema donante con Rescue and Recovery instalado, edite el archivo TVT.TXT ubicado en el directorio *C:\Archivos de programa\IBM\ThinkVantage*.
   - Cree una nueva sección `rescue` en el archivo TVT.TXT.
   - Añada la entrada siguiente a la sección rescue:

     ```
     mailbox=
     ```

     y, a continuación, añada la información del directorio del buzón de correo. Los buzones de correo en la unidad local, por ejemplo, deben tener el aspecto siguiente:

     ```
     [rescue]
     mailbox=C:\ADM\Mailbox,
      \\Network\Share
     ```

     Los buzones de correo en un sitio FTP tendrían un aspecto similar al siguiente:

     ```
     ftp://ftp.buzóndecorreo.com
     ```

     Los buzones de correo en una unidad de red compartida tendrían un aspecto como el siguiente:

     ```
     \\Red\Compartición
     ```

     Notas:

     a. HTTPS no está soportado para las funciones de buzón de correo.
     b. Se debe configurar el servidor Web HTTP para que proporcione el indexado activado y liste la capacidad de los archivos.

     Las letras de las unidades pueden cambiar entre Windows Professional Edition y el entorno del sistema operativo normal. Con bastante probabilidad

la unidad C: cambiará. Para solucionar esto, utilice la variable de entorno *CUSTOS*, que siempre apunta a la unidad que contiene el sistema operativo del cliente típico. El ejemplo anterior cambiaría a:

```
mailbox=%CUSTOS%\ADM\Mailbox,ftp://ftp.buzóndecorreo.com, \\Red\Compartición
```

La serie de caracteres puede tener cualquier longitud mientras se adecue a los estándares del dispositivo o protocolo que se esté utilizando. Por ejemplo, si se está utilizando un archivo local, la vía de acceso no puede tener más de 256 caracteres.

- Varias entradas de correo están separadas por comas o signos de punto y coma.
- Antidote Delivery Manager busca secuencialmente los paquetes en las ubicaciones de los buzones de correo especificados.

3. Si son necesarios un nombre de usuario y una contraseña para una conexión FTP o HTTP, utilice este formato:

   ```
   ftp//nombreusuario:contraseña@ftp.buzóncorreos.com
   ```

4. Para el nombre de usuario y la contraseña de buzones de correo de comparticiones de red:

   Las entradas de nombre de usuario y contraseña se almacenan cifradas en el archivo TVT.TXT. Para añadir una entrada en el sistema donante:

   a. Abra una ventana de DOS
   b. Cambie el directorio a `C:\Archivos de programa\IBM ThinkVantage\Rescue and Recovery\ADM`
   c. Ejecute este mandato:

      ```
      auncpw /add \\Red\Compartición /usuario nombreusuario /pwd contraseña
      /ref refID
      ```

      Este mandato crea la siguiente entrada en el archivo TVT.TXT:

      ```
      [RscDrv0]
      UNC=\\Red\Compartición
       User=01E23397A54D949427D5AF69BF407D5C
      Pwd=04E22197B34D95943ED5A169A0407C5C
      Ref=refID
      ```

   Notas:

   a. Esta entrada se puede utilizar en cualquier sistema a fin de que la utilice Antidote Delivery Manager para acceder a la misma compartición.
   b. Antidote Delivery Manager puede utilizar hasta 10 comparticiones de red.
   c. Además de las 10 comparticiones de red, se pueden añadir otras entradas de buzón de correos, como por ejemplo FTP o local.
   d. El archivo AUNCPW.EXE tiene otras funciones que se pueden utilizar para la gestión de contraseña. Especifique AUNCPW /? en la línea de mandatos o consulte Tabla 59 en la página 185.

5. Cree el par de claves privada/pública de Antidote Delivery Manager. Le recomendados que utilice las capacidades del par de claves pública/privada de Antidote Delivery Manager. Antidote Delivery Manager utiliza un par de claves pública/privada para verificar la autenticidad de los paquetes. La clave privada se debe guardar cuidadosamente y no se debe distribuir. La clave pública coincidente debe estar en cada cliente gestionado mediante Antidote Delivery Manager. Para crear un par de claves pública/privada en un sistema no donante con Rescue and Recovery instalado:

   a. Abra una ventana de DOS.
   b. Emita un mandato CD a C:\Archivos de programa\IBM ThinkVantage\Rescue and Recovery\ADM.

c. Ejecute este mandato:

```
apkgmes.exe /nuevaclave miclave
```

Este mandato crea dos archivos, mykey.pub y mykey.prv, que son la clave pública y la clave privada, respectivamente.

d. Copie la clave pública en el directorio C:\Archivos de programa\IBM ThinkVantage\Rescue and Recovery\ADM del sistema donante.

e. Abra el archivo utilizando un programa de edición de texto como por ejemplo notepad.exe.

f. Copie el contenido del archivo en el portapapeles.

g. En la línea de mandatos, especifique lo siguiente:

```
apubkey.exe /add x
```

donde *x* es el contenido del portapapeles.

h. Esto creará una entrada en el archivo TVT.TXT en la sección [rescue]: `pubkey0=906253....`

- Se pueden almacenar hasta 10 claves públicas en el archivo TVT.TXT.
- El archivo APUBKEY.EXE tiene otras funciones que se pueden utilizar para la gestión de claves públicas. En la línea de mandatos, especifique `APUBKEY /?` o consulte Tabla 59 en la página 185.

6. Cree la comprobación de planificación de Antidote Delivery Manager (se permiten múltiples planificaciones). Es necesario ejecutar Antidote Delivery Manager periódicamente en el sistema. Para configurar que una planificación se ejecute cada 20 minutos, se debe añadir lo siguiente al archivo TVT.TXT en el sistema donante:

```
[Scheduler]
Task1=rescuerecovery
Task2=egatherer
Task3=rescue

[rescue]
ScheduleFrequency=0
ScheduleMode=0x01
NumMinutes=20
TaskShow=1
Task=C:\Archivos de programa\IBM ThinkVantage\Rescue and Recovery\ADM\antidote
\mailman.exe
```

donde *ScheduleMode* es el suceso que activará la entrega del paquete de Antidote Delivery Manager. Los parámetros son los siguientes:

Tabla 62. Parámetros de Antidote Delivery Manager

Parámetro	Valor
SCHED_NONE	0x000
SCHED_MINUTELY	0x001
SCHED_DAILY	0x002
SCHED_WEEKLY	0x004
SCHED_MONTHLY	0x008
SCHED_STARTUP	0x010
SCHED_WAKEUP	0x020
SCHED_USB_ATTACH	0x040
SCHED_NETWORK_ATTACH	0x080

Notas:

a. El planificador no se ejecuta en el Área previa al escritorio.

b. Para obtener más información, consulte “Planificación de copias de seguridad y tareas relacionadas” en la página 160.

7. Cree un paquete de Antidote Delivery Manager.

   Cuando haya completado los pasos anteriores, cree y distribuya el primer paquete. En un sistema de administrador (no donante), realice los pasos siguientes:

   a. Cree un directorio como por ejemplo *C:\ADM\Build*.

   b. En ese directorio, cree un archivo denominado GO.RRS y añada lo siguiente:

      ```
      msgbox.exe /msg "Hola gente" /head "test" /ok /cancel
      ```

   c. Guarde y cierre el archivo.

   d. Emita un mandato CD a C:\Archivos de programa\IBM ThinkVantage\Rescue and Recovery\ADM

   e. Ejecute este mandato:

      ```
      apkgmes.exe /key mykey.prv C:\adm\build HELLOPKG
      ```

   f. Esto creará un paquete denominado HELLOPKGYY*MMDDHHMM*.ZAP donde *MMDDHHMM* será sustituido por la fecha/hora actual.

8. Copie el archivo HELLOPKGYY*MMDDHHMM*.ZAP en una ubicación de buzón de correo especificada en el paso 2.

9. Invoque a Antidote Delivery Manager.

   a. Cuando el temporizador haya caducado en el sistema donante, se ejecutará el paquete y se visualizará un mensaje Hola gente.

   b. Si prefiere no tener que esperar, en el sistema donante puede entrar C:\Archivos de programa\IBM ThinkVantage\Rescue and Recovery\ADM\mailman.exe

Ejemplos

A continuación se muestran algunos ejemplos de la forma de utilizar Antidote Delivery Manager:

Ejemplo 1

Este ejemplo es un paquete para arreglar un sistema que visualiza constantemente una pantalla azul debido a un virus o a una entrada errónea en el registro.

1. Asuma que la razón por la que el sistema cliente está visualizando una pantalla azul es debido a un virus que se ejecuta mediante la Clave de ejecución en el registro. Para arreglar esto, es necesario crear un archivo denominado go.rrs que ejecuta *reg*. Consulte “Mandatos de Microsoft soportados” en la página 189 para ver una lista de mandatos de Microsoft. Reg elimina el valor del registro y suprime el ejecutable del sistema, si es posible. El contenido debe tener el siguiente aspecto:

   ```
   reg delete HKLM\Software\Microsoft\Windows\Current Version\Run /v runvirusvalue
   /f del %custos%\windows\system32\virus.exe
   ```

2. A continuación, coloque el archivo go.rrs en el directorio *c:\adm\build* y ejecute:

   ```
   apkgmes.exe /key mykey.prv C:\adm\build REMOVEVIRUS
   ```

3. Copie REMOVEVIRUS*AADDHHMM*.ZAP en el buzón de correo.

4. Arranque cada cliente y pulse el botón Access IBM/F11 o la tecla Intro para entrar en el Área previa al escritorio donde se ejecuta el archivo mailman.exe al arrancar y, a continuación, ejecute el paquete REMOVEVIRUS.

Ejemplo 2

Este ejemplo hace que se descargue en las máquinas cliente la actualización o el parche de Quick Fix Engineering.

1. Cree un directorio donde albergar el archivo script y los archivos de parche, como por ejemplo *C:\adm\patchbuild*.
2. Coloque el ejecutable de qfe o del parche en el directorio c:\adm\patchbuild.
3. Cree un archivo denominado go.rrs y coloque las líneas siguientes en el mismo para personalizar la línea que ejecutará e instalará el parche o Quick Fix Engineering de Microsoft Quick Fix Engineering. Debido a que este parche sólo se puede instalar en un sistema operativo Windows normal, este script impide que la instalación se intente ejecutar en Windows Professional Edition.

   ```
   set custos
   if errorlevel 1 set custos=%systemDrive%
   %custos%\Archivos de programa\IBM ThinkVantage\Rescue and Recovery\ADM\
   retryonerror /on 10
   %custos%\Archivos de programa\IBM ThinkVantage\Rescue and Recovery\ADM\InRR.exe
   if errorlevel 2 goto ERROR
   if errorlevel 1 goto InOS
   if errorlevel 0 goto InPE

   :ERROR
   exit 1

   :InOS
   REM DISABLE NETWORKING
   Netwk.exe /d
   patchinstall.exe
   REM ENABLE NETWORKING
   Netwk.exe /e
   msgbox.exe /msg "Patch Installed" /head "Done" /ok
   exit 0

   :InPE
   exit 1
   ```

4. Coloque el archivo go.rrs en el directorio c:\adm\patchbuild y ejecute:

   ```
   apkgmes.exe /key mykey.prv C:\adm\patchbuild PATCHBUILD
   ```

5. Copie PATCHBUILD*AADDHHMM*.ZAP en el buzón de correo.
6. El parche se instalará durante la siguiente ejecución planificada del archivo mailman.exe para la máquina cliente o durante el rearranque de la máquina cliente.

Formas de comprobar si el paquete está completo

- **Fail.log**

  Este archivo se almacena normalmente en el directorio *c:\ibmtools\utils\rescue*. Si el archivo zap existe con un valor distinto de cero, quedará registrado en este archivo.

- **Rescue.log**

  Este archivo se almacena normalmente en el directorio *c:\ibmshare*. Este archivo proporciona información más detallada que puede ayudarle a determinar por qué un paquete ha fallado, o para asegurar se que un paquete ha funcionado. Tiene un registro línea a línea de lo que sucede en un archivo zap.

- **Success.log**

  Este archivo se almacena normalmente en el directorio *c:\ibmtools\utils\rescue*. Si un archivo zap ha salido con un valor de cero, quedará registrado aquí.

Ejemplo 3

Este ejemplo utiliza un sitio FTP o HTTP en el Área previa al escritorio:

1. Defina un sitio Web externo para los paquetes:

   ```
   ftp.buzóndecorreo.com
   ```

2. Cree claves privadas/públicas.
3. Añada el buzón de correo a TVT.TXT

   ```
   mailbox=ftp://nombreusuario:contraseña@ftp.buzóncorreos.com
   ```

4. Cuando el usuario pulsa Access IBM/F11 o la tecla Intro para entrar en el Área previa al escritorio, el paquete de Antidote Delivery Manager se ejecuta durante el arranque en el Área previa al escritorio.

Ejemplo 4

Este ejemplo utiliza el archivo xmltool.exe para alcanzar algunos clientes:

1. Distribuya el archivo xml que tiene información en el mismo que desea que se compare en las máquinas clientes, bien mediante Active Directory, Systems Management Server o alguna otra herramienta de gestión.

   ```
   <file>
   <activedirgroup>Marketing</activedirgroup>
   </file>
   ```

2. En la primera línea del archivo go.rrs, coloque una línea que utiliza la herramienta xml. Esta línea es un ejemplo que SÓLO tendría como destino máquinas del grupo Marketing;

   ```
   xmltool.exe c:\miempresa\target.xml //file/activedirgroup /c EQU Marketing
   if errorlevel 0 goto RUNIT
   exit errorlevel

   :RUNIT
   #coloque el código para ejecutar el parche u otra acción
   ```

Ataque importante de gusanos

El ejemplo siguiente muestra un posible procedimiento para combatir un virus importante. El procedimiento básico es desactivar las comunicaciones de red y, a continuación, reiniciar en Rescue and Recovery, reparar el registro, copiar el archivo de sustitución en su sitio, arrancar de nuevo en Windows XP y restaurar las comunicaciones de red. A modo de este ejemplo, es necesario realizar la siguiente aplicación a fin de revisar la sintaxis.

Go.RRS

```
set tagfile=1.tag
set pingtarg=192.168.1.1
retryonerror /on 10
set custos
if errorlevel 1 set custos=%systemDrive%

cd %custos%\ibmtools\utils\rescue\dne\work

inRR.exe
if errorlevel 2 goto ERROR
if errorlevel 1 goto InOS
if errorlevel 0 goto inRR

:InOS
cd
if exist %tagfile% goto DONE

msgbox /msg "Antidote ha detectado un nuevo mensaje \n  \n ..... \n  \n No se preocupe: sea feliz
```

```
Antidote arreglará el sistema para usted" /ok /timer 30
call nettest.cmd %pingtarg%
set el=%errorlevel%
if %el% == 0 msgbox /msg "La red está funcionando" /timer 5 /head "Correcto"
if not %el% == 0 msgbox /msg "La red está inhabilitada" /timer 5 /head "Fallo"
NetWk.exe /d
msgbox.exe /msg "Se está ejecutando el proceso de recuperación de Antidote. \n  \n
Se han inhabilitado las comunicaciones de red." /head
"Comunicaciones de red" /timer 15
call nettest.cmd %pingtarg%
set el=%errorlevel%
if %el% == 0 msgbox /msg "La red está funcionando" /timer 5 /head "Fallo"
if not %el% == 0 msgbox /msg "La red está inhabilitada" /timer 5 /head "Correcto"
msgbox.exe /msg "El sistema rearrancará en 20 segundos \n  \n Pulse Aceptar para rearrancar ahora
o Cancelar para rearrancar más tarde."
/head "Seleccione Reparación de emergencia" /timer 20 /ok /cancel
if errorlevel 2 goto PENOW
if errorlevel 1 goto PELATER
if errorlevel 0 goto PENOW

:PENOW
reboot /rr
goto NOT_DONE


:PELATER
%custos%\ibmtools\utils\bmgr32.exe /bw
msgbox.exe /msg "El sistema aplicará el arreglo la próxima vez que rearranque" /head "Rearranque" /ok
goto NOT_DONE

:inRR
REM DISABLE NETWORKING
msgbox.exe /msg "Las comunicaciones de red se inhabilitarán dentro de 5 segundos. \n  \n
"Pendiente la inhabilitación de la red"
/head "Cierre de la red" /timer 5
NetWk.exe /d

REM USE EGATHERER VALUES FOR CONDITIONAL BRANCH

msgbox /msg "Comprobando el registro" /timer 5
xmltool %ibmshare%\ibmegath.xml //EG_GATHERED_DATA/EG_INSTALLED_MICROSOFT_SOFTWARE/
EG_SOFTWARE_PACKAGE[@ID='DirectX']/EG_VERSION GEQ \"4.09.00.0901\"
if errorlevel 1 goto FILECOPY

msgbox.exe /msg "Aplicando el arreglo del registro. \n  \n Pulse Aceptar para continuar..." /head
"Arreglo del registro" /ok
reg.exe load HKLM\tempSW %custos%\windows\system32\config\SOFTWARE
reg.exe add "HKLM\tempSW\IBM\eGatherer\Local Viewer\scans\banka" /v benke /d binki /f
reg.exe add "HKLM\tempSW\IBM\eGatherer\Local Viewer\scans\banka" /v bonko /d bunku /f
reg.exe delete "HKLM\tempSW\IBM\eGatherer\Local Viewer\scans\banka" /v bonko /f
reg.exe unload HKLM\tempSW

:FILECOPY
msgbox /msg "El registro ahora está bien \n  \n Aplicando arreglo" /timer 5
copy payload.txt %custos%\

REM RE-ENABLE NETWORK
msgbox.exe /msg "Las comunicaciones de red se habilitarán dentro de 5 segundos. \n  \n
Pendiente la habilitación de la red" /head
"Cierre de la red" /timer 5
NetWk.exe /e

REM TAG IT
echo 1 > %tagfile%

REM REBOOT
msgbox.exe /msg "El sistema rearrancará dentro de 5 segundos..." /head "Rearranque..." /timer 5
```

```
reboot.exe
goto NOT_DONE

:ERROR
:NOT_DONE
exit 1

:DONE
NetWk.exe /e
msgbox.exe /msg "Se ha aplicado el arreglo \n  \n Puede continuar el funcionamiento normal."
/head "Hecho" /ok
exit 0
```

NETTEST.CMD

```
PING –n 1 %1 > nul 2>&
```

PAYLOAD.TXT

```
un archivo de prueba
de una carga a entregar.
```

Apéndice G. Avisos

Es posible que Lenovo no ofrezca todos los productos, servicios o características descritos en este documento en todos los países. Consulte al representante local de Lenovo para obtener información acerca de los productos y servicios que están actualmente disponibles en su área. Cualquier referencia a un producto, programa o servicio de Lenovo no pretende indicar o implicar que sólo se pueda utilizar dicho producto, programa o servicio de Lenovo. En su lugar, se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no infrinja el derecho de propiedad intelectual de Lenovo. Sin embargo, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

Lenovo puede tener patentes o solicitudes de patente pendientes que traten el tema descrito en este documento. El suministro de este documento no le proporciona ninguna licencia sobre estas patentes. Puede enviar preguntas sobre licencias, por escrito, a:

Lenovo (United States), Inc
500 Park Offices Drive, Hwy 54
Research Triangle Park, NC 27709
EE.UU.
A la atención de: Lenovo Director of Licensing

LENOVO GROUP LTD. PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL", SIN GARANTÍAS DE NINGÚN TIPO, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUYENDO, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO VIOLACIÓN, MERCANTIBILIDAD O ADECUACIÓN A UN PROPÓSITO DETERMINADO. Algunas jurisdicciones no permiten la renuncia a garantías implícitas o explícitas en algunas transacciones; por lo tanto, es posible que esta declaración no sea aplicable en su caso.

Esta información podría incluir imprecisiones técnicas o errores tipográficos. Periódicamente se realizan cambios en la información aquí contenida; estos cambios se incorporarán en nuevas ediciones de la publicación. Lenovo puede realizar mejoras y/o cambios en los productos y/o los programas descritos en esta publicación en cualquier momento sin aviso previo.

Los productos descritos en este documento no están destinados a la utilización en la implementación u otras aplicaciones de soporte vital cuyo funcionamiento incorrecto pueda dar como resultado el daño o la muerte de personas. La información contenida en este documento no afecta ni cambia las especificaciones ni las garantías del producto Lenovo. No hay nada en este documento que funcione como una licencia ni indemnización explícita ni explícita bajo los derechos de propiedad intelectual de Lenovo y de terceros. Toda la información contenida en este documento se ha obtenido en entornos específicos y se presenta como ejemplo. El resultado obtenido en otros entornos operativos puede variar.

Lenovo puede utilizar o distribuir cualquier información que el usuario proporcione de cualquier manera que crea conveniente sin incurrir por ello en ninguna obligación con el usuario.

Cualquier referencia realizada en esta publicación a sitios Web que no sean de Lenovo se proporciona sólo para su comodidad y de ninguna manera sirven como

una aprobación de dichos sitios Web. Los materiales de estos sitios Web no forman parte de los materiales para este producto Lenovo, y la utilización de estos sitios Web la realiza el usuario por su propia cuenta y riesgo.

Los datos de rendimiento aquí contenidos se han obtenido en un entorno controlado. Por lo tanto, el resultado en otros sistemas operativos puede variar de forma significativa. Algunas mediciones se han realizado en sistemas a nivel de desarrollo y no hay ninguna garantía que de estas mediciones sean las mismas en sistemas disponibles comercialmente. Además, algunas mediciones se han realizado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables para su entorno específico.

Marcas registradas

Los términos siguientes son marcas registradas de Lenovo en Estados Unidos y/o en otros países:

Lenovo
Rescue and Recovery
ThinkPad
ThinkCentre
ThinkVantage
Rapid Restore

Intel es una marca registrada de Intel Corporation o sus subsidiarios en Estados Unidos y en otros países.

Los términos siguientes son marcas registradas de International Business Machines Corporation en Estados Unidos y/o en otros países: IBM, Lotus y Lotus Notes.

Microsoft, Windows y Windows NT son marcas registradas de Microsoft Corporation en los Estados Unidos y/o en otros países.

Es posible que otros nombres de empresas, productos o servicios sean marcas registradas o de servicio de otros.

Glosario

Advanced Encryption Standard (AES). *Advanced Encryption Standard* es una técnica de cifrado de *claves simétricas*. El gobierno de los EE.UU. adoptó el algoritmo como su técnica de cifrado en octubre de 2000, sustituyendo el cifrado DES que utilizaba. AES ofrece una mayor seguridad contra los ataques de fuerza bruta que las claves a 56 bits, y AES puede utilizar claves de 128, 192 y 256 bits, si es necesario.

Chip de seguridad incorporado. El chip de seguridad incorporado es otro nombre para un Módulo de plataforma fiable.

Cifrado de claves públicas/claves asimétricas. Los algoritmos de claves públicas normalmente utilizan un par de dos claves relacionadas — una clave es privada y se debe mantener en secreto, mientras que la otra se hace pública y se puede distribuir ampliamente; no debe ser posible deducir una clave de un par si se proporciona la otra. La terminología de ″cifrado de claves púbicas″ deriva de la idea de hacer parte de la clave información pública. El término cifrado de claves asimétricas también se utiliza porque no todas las partes mantienen la misma información. En cierto sentido, una clave ″bloquea″ un bloqueo (cifra); pero es necesario una clave distinta para desbloquearla (descifrarla).

Cifrado de claves simétricas. Las cifras del cifrado de claves simétricas utilizan la misma clave para cifrar y para descifrar los datos. Las cifras de las claves simétricas son más simples y más rápidas, pero su principal desventaja es que las dos partes deben de alguna manera intercambiar la clave de una forma segura. El cifrado de claves públicas evita este problema porque la clave pública se puede distribuir de una forma no segura, y la clave privada no se transmite nunca. Advanced Encryption Standard es un ejemplo de una clave simétrica.

Clave raíz de almacenamiento (SRK). La clave raíz de almacenamiento (SRK) es un par de claves públicas de 2,048 bits (o más grande). Está inicialmente vacía y se crea cuando se asigna el propietario del TPM. Este par de claves nunca abandona el chip de seguridad incorporado. Se utiliza para cifrar (empaquetar) claves privadas para el almacenamiento fuera del Módulo de plataforma fiable y para descifrarlas cuando se cargan de nuevo en el Módulo de plataforma fiable. La SRK la puede borrar cualquiera que tenga acceso al BIOS.

Contraseña del BIOS de Administrator (ThinkCentre) / Supervisor (ThinkPad). La contraseña de administrador o de supervisor se utiliza para controlar la capacidad de cambiar los valores del BIOS. Esto incluye la capacidad de habilitar/inhabilitar el chip de seguridad incorporado y de borrar la Clave raíz de almacenamiento almacenada en el Módulo de plataforma segura.

Módulo de plataforma fiable (TPM). Los Módulos de plataforma fiable son circuitos integrados con un propósito especial incorporados en los sistemas para permitir una autentificación de usuario y verificación de la máquina fuertes. La finalidad principal del TPM es evitar el acceso inadecuado a información importante y confidencial. El TPM es una raíz de fiabilidad basada en hardware que se puede aprovechar para proporcionar una variedad de servicios de cifrado en un sistema. Otro nombre para el TPM es el chip de seguridad incorporado.

Sistemas de cifrado. Los sistemas de cifrado se pueden clasificar ampliamente en cifrado de claves simétricas que utilizan una única clave que cifra y descifra los datos, y cifrado de claves públicas que utiliza dos claves, una clave pública conocida por todo el mundo y una clave privada a la que sólo tiene acceso el propietario del par de claves.

ThinkVantage

Número Pieza: 41R9860

Impreso en España

(1P) P/N: 41R9860