ThinkVantage

ThinkVantage Technologies: Guia de Implementação

Atualizado em: 29 de Setembro de 2005

Inclui:

- Rescue and Recovery Versão 3.0
- Client Security Solution Versão 6.0
- Fingerprint Software Versão 4.6

ThinkVantage

ThinkVantage Technologies: Guia de Implementação

Atualizado em: 29 de Setembro de 2005

Primeira Edição (Setembro de 2005)

Índice

Prefácio

Este guia destina-se a administradores de TI ou responsáveis pela implementação do programa Rescue and Recovery em todos os computadores da organização. A finalidade do Rescue and Recovery é reduzir custos, permitindo chamadas ao helpdesk e visitas ao deskside e aprimorar a produtividade do usuário. É uma ferramenta essencial que permite que usuários e administradores restaurem backups, arquivos de acesso, diagnostiquem problemas e estabeleçam conexões com a Ethernet, caso o sistema operacional Microsoft® Windows não abra ou execute corretamente. Permite também a implementação de atualizações críticas em sistemas corrompidos ou fora da rede, bem como a aplicação automática de correções ao sistema quando uma restauração for executada. Este guia fornece as informações necessárias para a instalação do aplicativo Rescue and Recovery em um ou vários computadores, desde que licenças de software estejam disponíveis em cada computador de destino e informações sobre vários aspectos da ferramenta possam ser customizadas para suportar políticas corporativas ou de TI. Para perguntas e informações sobre como utilizar os diversos componentes incluídos no espaço de trabalho do Rescue and Recovery, consulte o sistema de ajuda on-line dos componentes.

O Rescue and Recovery fornece ajuda a funções e ao aplicativo. Para perguntas e informações sobre como utilizar os diversos componentes incluídos no espaço de trabalho do Rescue and Recovery, consulte o sistema de ajuda on-line dos componentes.

Este guia de implementação é desenvolvido por profissionais de TI e os desafios exclusivos que eles enfrentam. Se você tiver sugestões ou comentários, comunique-se com o seu representante autorizado Lenovo. Estes guias são atualizados periodicamente, portanto verifique este Web site para obter versões posteriores:

www.lenovo.com/ThinkVantage

Capítulo 1. Visão Geral

O público deste guia é pessoal de Segurança e Administração de TI e outras pessoas que sejam responsáveis pela implementação e implantação de tecnologia de segurança em uma corporação. O ThinkVantage Rescue and Recovery representa uma combinação única das Tecnologias ThinkVantage. Esse aplicativo integrado fornece um conjunto de ferramentas eficazes que podem ser utilizadas mesmo se o sistema operacional Microsoft Windows não for iniciado.

No ambiente corporativo, essas tecnologias podem ajudar direta e indiretamente os profissionais de TI. Todas as Tecnologias ThinkVantage beneficiarão os profissionais de TI porque elas ajudam a tornar os computadores pessoais mais fáceis de utilizar e mais auto-suficientes, e fornecem ferramentas poderosas que facilitam e simplificam as implementações. Em uma base contínua, as Tecnologias do ThinkVantage ajudam os profissionais de TI a economizar tempo na resolução de problemas individuais do computador para dedicar mais tempo às tarefas principais.

Componentes Principais

Os componentes principais deste guia são:

- ThinkVantage Rescue and Recovery
- ThinkVantage Client Security Solution
- ThinkVantage Fingerprint Software

Uma discussão sobre cada um deles é apresentada a seguir.

Rescue and Recovery

O Rescue and Recovery tem dois componentes principais:

- O ambiente Pré-desktop do Rescue and Recovery é iniciado mesmo se o sistema operacional Windows não inicializar.
- O ambiente Windows do Rescue and Recovery permite o backup, resgate de arquivos e recuperação do sistema operacional e de arquivos.

Nota: Alguns recursos do Rescue and Recovery são executados no sistema operacional Windows. Em algumas instâncias, as informações sobre o sistema utilizadas no ambiente do Rescue and Recovery são reunidas durante a execução do Windows. Se o sistema operacional Windows não funcionar corretamente, apenas esse mau funcionamento não impedirá que o ambiente do Rescue and Recovery opere normalmente. No entanto, as funções executadas no sistema operacional Windows não serão configuráveis e, por essa razão, essas funções não serão tratadas neste guia de implementação.

Ambiente Pré-desktop do Rescue and Recovery

O ambiente do Rescue and Recovery fornece um espaço de trabalho de emergência para usuários finais que não conseguem iniciar o Windows em seus computadores. Ao executar no PE (Ambiente de Pré-instalação) do Windows, o ambiente oferece a aparência, a impressão e a funcionalidade do Windows e ajuda os usuários finais a resolver os problemas sem consumir o tempo da equipe de TI.

O ambiente do Rescue and Recovery tem quatro categorias principais de funções:

- **Resgatar e Restaurar**
  - **Visão Geral da Recuperação:** Leva os usuários a tópicos da ajuda sobre as diversas opções de recuperação oferecidas.
  - **Arquivos de Resgate:** Permite que os usuários copiem arquivos criados em aplicativos Windows para mídia removível ou para uma rede e continue a funcionar mesmo com uma estação de trabalho desativada.
  - **Restauração a Partir de Backup:** Permite que os usuários restaurem arquivos cujo backup foi feito com o Rescue and Recovery.
- **Configurar**
  - **Visão Geral da Configuração:** Vincula o ambiente do Rescue and Recovery aos tópicos da ajuda que abrangem a configuração.
  - **Recuperar Senha/Passphrase:** Fornece a um usuário ou administrador a capacidade de recuperar uma senha ou passphrase no ambiente do Rescue and Recovery.
  - **Acessar BIOS:** Abre o programa BIOS Setup Utility.
- **Comunicar**
  - **Visão Geral da Comunicação:** Vincula aos tópicos da ajuda relacionados no ambiente do Rescue and Recovery.
  - **Abrir Navegador:** Inicia o navegador da Web Opera (o acesso à Web ou à Intranet requer uma conexão Ethernet com conexão física).
  - **Fazer Download de Arquivos**
  - **Mapear a Unidade de Rede:** Ajuda os usuários finais a acessar unidades de rede para fazer download de softwares ou transferir arquivos.
- **Resolução de Problemas**
  - **Visão Geral do Diagnóstico:** Vincula aos tópicos de ajuda de diagnósticos do Rescue and Recovery.
  - **Diagnosticar Hardware:** Abre o aplicativo PC Doctor que pode executar testes de hardware e relatar resultados.
  - **Criar Discos de Diagnósticos**
  - **Inicializar de Outro Dispositivo**
  - **Informações sobre o Sistema:** Fornece detalhes a respeito do computador e seus componentes de hardware.
  - **Registro de Eventos:** Fornece detalhes sobre atividades recentes do usuário e listagens de hardware do computador para auxiliar na determinação e resolução de problemas. O visualizador do log fornece uma maneira legível de visualizar a atividade e as entradas do log de recursos.
  - **Status de Garantia**

O Rescue and Recovery está disponível em computadores pessoais das marcas IBM e Lenovo fornecidos com software pré-instalado. Também está disponível para aquisição como um arquivo que pode ser transferido por download para que as organizações possam beneficiar-se do Rescue and Recovery também em computadores de outras marcas.

O Apêndice B, “Configurações e Valores do TVT.TXT”, na página 141 trata da configuração do ambiente do Rescue and Recovery para implementação. Embora a instalação do Rescue and Recovery inclua a instalação do Rapid Restore Ultra, este guia os trata como componentes individuais nas descrições de personalização, configuração e implementação.

O Ambiente Windows do Rescue and Recovery

O ambiente do Rapid Restore permite que usuários finais resgatem dados, aplicativos e sistemas operacionais perdidos com o toque de um botão. Esse recurso reduz o tempo gasto em chamadas ao help-desk, o que resulta em economia no custo de suporte.

Você pode planejar backups de todos os computadores de usuários finais, limitando, assim, o risco e o tempo de inatividade. O Rescue and Recovery oferece aos clientes uma camada extra de suporte por meio da pré-configuração de backup externo automático para um servidor ou para armazenamento externo.

Antidote Delivery Manager

O Antidote Delivery Manager é uma infra-estrutura antivírus e antiworm incluída no ThinkVantage Rescue and Recovery. Os objetos são fáceis de implementar, eficientes e permitem que um administrador inicie o bloqueio e a recuperação em minutos quando um problema é relatado. Ele pode ser ativado por um administrador e funciona em sistemas que não estejam conectados à rede. O Antidote Delivery Manager complementa as ferramentas antivírus existentes em vez de substituí-las, portanto, a manutenção das ferramentas para varredura de vírus e a obtenção de correções continua sendo necessária. O Antidote Delivery Manager fornece a infra-estrutura para interromper a destruição e aplicar as correções.

Criptografando Backups

Os backups são criptografados por padrão com a chave 256 AES. Se você optar por instalar o Client Security Solution Versão 6.0, terá a capacidade de criptografar utilizando o Client Security Software Gina.

Client Security Solution 6.0

A finalidade principal do software Client Security Solution é ajudar um cliente a proteger o PC como patrimônio, proteger dados confidenciais no PC e proteger conexões de rede acessadas pelo PC. Para sistemas das marcas IBM e Lenovo que contenham um TPM (Trusted Platform Module) em conformidade com o TCG (Trusted Computing Group), o software CSS (Client Security Solution) alavancará o hardware como a raiz de confiança para o sistema. Se o sistema não contiver um chip de segurança integrado,o Client Security Solution alavancará chaves criptográficas baseadas em software como a raiz de confiança para o sistema. Os recursos do Client Security Solution 6.0 incluem:

- **Autenticação de Usuário Segura**

  Exige uma passphrase protegida por hardware do Client Security para que os usuários acessem funções protegidas do Client Security Solution.
- **Autenticação de Usuário por Impressão Digital**

  Alavanca a tecnologia de impressão digital integrada e conectada por USB para autenticar usuários para aplicativos protegidos por senha.
- **Logon do Client Security no Windows Baseado em Passphrase / Impressão Digital**

  Exige que os usuários efetuem logon no Windows utilizando sua passphrase do Client Security protegida por hardware ou impressão digital.
- **Proteção de Dados**

Criptografa arquivos sensíveis armazenando-os em um local protegido na unidade de disco rígido que exige autenticação de usuário válida e um chip de segurança configurado corretamente.

- **Gerenciamento de Senhas de Usuário**

  Gerencia e armazena com segurança informações sensíveis de logon, tais como IDs de usuários e senhas.

- **Recuperação de Senha/Passphrase de Usuário Final**

  Permite que os próprios usuários se recuperem de um senha / passphrase esquecida do Client Security no Windows respondendo a perguntas pré-configuradas.

- **Auditoria de Configurações de Segurança**

  Permite que os usuários visualizem uma lista detalhada de configurações de segurança da estação de trabalho e façam alterações para se enquadrarem em padrões definidos.

- **Transferência de Certificados Digitais**

  Protege por hardware a chave privada de certificados de Usuário e de Máquina.

Passphrase do Client Security

A passphrase do Client Security é uma forma adicional opcional de autenticação de usuário que fornecerá melhor segurança a aplicativos do Client Security Solution. A passphrase do Client Security tem os seguintes requisitos:

- Ter no mínimo oito caracteres de comprimento.
- Conter pelo menos um dígito.
- Ser diferente das três últimas passphrases.
- Não conter mais que dois caracteres repetidos.
- Não iniciar com um dígito.
- Não terminar com um dígito.
- Não conter o ID do usuário.
- Não ser alterada se a passphrase atual tiver menos de três dias de idade.
- Não conter três ou mais caracteres consecutivos idênticos aos da passphrase atual em nenhuma posição.
- Não ser igual à senha do Windows.

A passphrase do Client Security não é aceitável para o mesmo tipo de ataques que a senha do Windows. É importante observar que uma passphrase do Client Security somente é conhecida pelo usuário individual e a única maneira de recuperar-se de uma passphrase esquecida do Client Security é alavancar a função de recuperação de senha do Client Security. Se o usuário tiver esquecido as respostas a suas perguntas de recuperação, não haverá maneira de recuperar os dados protegidos pela passphrase do Client Security.

Recuperação de Senha do Client Security

Esta configuração adicional permite que usuários inscritos recuperem uma senha do Windows ou passphrase do Client Security esquecidas respondendo corretamente a três perguntas. Se esse recurso for ativado, durante a inscrição de usuários finais no Client Security cada usuário poderá selecionar três respostas a 10 perguntas pré-escolhidas. Se o usuário esquecer sua senha do Windows ou passphrase do Client Security, terá a opção de responder a essas três perguntas para reconfigurar sua senha ou passphrase.

Notas:

1. Quando se utiliza a passphrase do Client Security, essa é a única opção para recuperação de uma passphrase esquecida. Se o usuário esquecer a resposta a suas três perguntas, será forçado a executar novamente o assistente de inscrição e perderá todos os dados protegidos anteriores do Client Security.
2. Quando se utiliza o Client Security para proteger o ambiente Pré-desktop do Rescue and Recovery, a opção de Recuperação de Senha na verdade exibirá a passphrase do Client Security e/ou a senha do Windows do usuário. A causa disso é que o ambiente Pré-desktop não tem a capacidade de executar automaticamente uma alteração da senha do Windows. Esse comentário também é verdadeiro quando um usuário de domínio armazenado em cache localmente não conectado pela rede executar essa função no logon do Windows.

ThinkVantage Fingerprint Software

O objetivo das tecnologias biométricas de impressão digital oferecidas pela Lenovo é o de ajudar os clientes a reduzirem os custos associados ao gerenciamento de senhas, melhorar a segurança de seus sistemas e ajudar a cuidar da conformidade a regulamentos. Juntamente com nossos leitores de impressão digital, o ThinkVantage Fingerprint Software permite a autenticação de impressão digital em seu PC e na rede. A solução também se integra com o Client Security Solution Versão 6.0 oferecendo funcionalidade expandida. Você pode descobrir mais sobre as tecnologias de impressão digital da Lenovo e fazer download do software em:

www.thinkpad.com/fingerprint

O ThinkVantage Fingerprint Software oferece estas funções:

- **Recursos do Software Cliente**
  - **Substituir senha do Microsoft Windows**

    Substitua por sua impressão digital para acesso fácil, rápido e seguro ao sistema.
  - **Substituir senhas do BIOS (também conhecida como senha de ligação) e de unidade de disco rígido:** por sua impressão digital para melhorar a segurança e conveniência do logon.

    Substitua essas senhas por sua impressão digital para melhorar a segurança e conveniência do logon.
  - **Acesso de leitura única ao Windows:**

    Um usuário pode ter sua impressão digital lida UMA VEZ na inicialização para ganhar acesso ao BIOS E ao Windows, poupando tempo valioso.
  - **Integração com o Client Security Solution** para uso com o Password Manager do CSS e para alavancar o Trusted Platform Module. Os usuários podem ter suas impressões digitais lidas para acessar web sites e selecionar aplicativos.
- **Recursos do Administrador**
  - **Comutar Modos de Segurança:**

    Um administrador pode comutar entre os modos protegido e conveniente para modificar os direitos de acesso de usuários limitados.
  - **Console de Gerenciamento:**

    Ajuda os administradores permitindo a customização remota do Fingerprint Software por meio de uma interface de linha de comandos orientada por scripts.

- **Recursos de Segurança**
  - **Segurança de Software:**

    Protege gabaritos de usuário por meio de criptografia forte quando armazenados em um sistema e quando transferidos do leitor para o software.
  - **Segurança de Hardware:**

    Os leitores possuem um coprocessador de segurança que armazena e protege gabaritos de impressão digital, senhas de BIOS e chaves de criptografia.

Password Manager

O Password Manager do Client Security permite gerenciar e lembrar todas as informações de login sensíveis e fáceis de esquecer de aplicativos e Web sites, tais como IDs de usuários, senhas e outras informações pessoais. O Password Manager do Client Security armazena todas as informações por meio do chip de segurança integrado para que o acesso a seus aplicativos e Web sites permaneça totalmente protegido.

Isso significa que, em vez de ter que lembrar e fornecer uma grande quantidade de senhas individuais - todas sujeitas a diferentes regras e datas de expiração - você só precisa lembrar de uma senha/passphrase, fornecer sua impressão digital, ou uma combinação de elementos de identificação.

O Password Manager do Client Security permite executar as seguintes funções:

- **Criptografar todas as informações armazenadas por meio do chip de segurança integrado**

  O Password Manager do Client Security criptografa automaticamente todas as informações por meio do chip de segurança integrado. Isso assegura que todas as informações sensíveis de senhas sejam protegidas pelas chaves de criptografia do Client Security Solution.
- **Transferir IDs de usuários e senhas rapidamente e facilmente utilizando uma interface simples de digitar e transferir**

  A interface de digitar e transferir do Password Manager do Client Security permite colocar as informações diretamente na interface de logon de seu navegador ou aplicativo. Isso ajuda a minimizar erros de digitação e permite salvar todas as informações com segurança por meio do chip de segurança integrado.
- **Digitar automaticamente IDs de usuários e senhas**

  O Password Manager do Client Security automatiza o processo de login, inserindo as informações de login automaticamente quando você acessar um aplicativo ou Web site cujas informação de logon tiverem sido inseridas no Password Manager do Client Security.
- **Gerar senhas aleatórias**

  O Password Manager do Client Security permite gerar senhas aleatórias para cada aplicativo ou Web site. Isso permite que você aumente a segurança de seus dados porque cada aplicativo terá uma proteção de senha muito mais rigorosa ativada. Senhas aleatórias são muito mais seguras que senhas definidas pelo usuário porque a experiência indica que a maioria dos usuários utiliza informações pessoais fáceis de lembrar como senhas que freqüentemente são fáceis de descobrir.
- **Editar entradas utilizando a interface do Password Manager do Client Security**

O Password Manager do Client Security permite editar todas as entradas de sua conta e configurar todos os recursos de senha opcionais em uma interface de fácil utilização. Isso torna rápido e fácil o gerenciamento das senhas e informações pessoais.

- **Acessar as informações de logon da bandeja de ícones no desktop do Microsoft(R) Windows(R) o com um atalho de teclado simples**

  O ícone do Password Manager concede acesso fácil a suas informações de logon sempre que for necessário incluir outro aplicativo ou Web site no Password Manager. Cada função do Password Manager do Client Security também pode ser facilmente acessada por um atalho de teclado simples.

- **Exportar e importar informações de login**

  O Password Manager do Client Security permite exportar suas informações sensíveis de login para que você possa transportá-las facilmente de um computador para outro. Ao exportar informações de login do Password Manager do Client Security, um arquivo de exportação protegido por senha é criado, o qual pode ser armazenado em mídia removível. Utilize esse arquivo para acessar suas informações de usuário e senhas onde quer que você vá, ou para importar suas entradas para outro computador com o Password Manager.

  Nota: A importação funcionará somente com o Client Security Solution Versão 6.0. O Client Security Software Versão 5.4X e versões anteriores não importarão para o Password Manager do Client Security Solution 6.0.

SafeGuard PrivateDisk

Proteja os dados usando o SafeGuard PrivateDisk. Quase todas as pessoas armazenam dados confidenciais em seus PCs. O SafeGuard PrivateDisk protege os dados confidenciais. Ele funciona como um "cofre eletrônico" para informações confidenciais e valiosas no computador, em todas as unidades de disco e em mídia portátil. As informações protegidas não podem ser acessadas ou lidas por pessoas não autorizadas.

Como o SafeGuard PrivateDisk funciona? O SafeGuard PrivateDisk se baseia no princípio de Disco Virtual.

- Um disco virtual pode ser criado em qualquer unidade disponível.
  - Mídia de memória portátil (tal como disco, sticks USB, CD-ROM, DVD ou Zip drive).
  - Unidades de disco rígido, unidades de rede.
- O driver opera como uma unidade de disco rígido
  - O sistema operacional envia comandos de gravação e leitura ao driver transparentemente.
  - O driver gerencia o armazenamento criptografado.
  - Todos os dados e informações de diretórios são criptografados.
- O SafeGuard PrivateDisk trabalha com o Client Security Solution e o Trusted Platform Module para proteger certificados digitais gerados pelo PrivateDisk
- O SafeGuard PrivateDisk utiliza um algoritmo de cifra simétrica com uma nova chave AES aleatória para cada disco virtual
  - AES, 128 Bits, modo CBC.
  - Nova chave aleatória para cada disco virtual.
- Autenticação por meio de:
  - Senha.
  - Chave Privada (certificado X.509), smartcard opcional.

- O uso de certificados EFS gerados automaticamente é possível.

- Segurança de senha:
  - PKCS#5.
  - Retardo após apresentação de senha incorreta.
  - Diálogo de senha com "proteção contra interceptação".

Security Advisor

A ferramenta Security Advisor permite visualizar um resumo da configurações de segurança definidas atualmente em seu computador. Você pode revisar essas configurações para visualizar o status atual da segurança ou para melhorar a segurança do sistema. Alguns dos tópicos de segurança incluídos são senhas de hardware, senhas de usuários do Windows, política de senhas do Windows, proteção de tela protegida e compartilhamento de arquivos. Os valores padrão das categorias exibidas podem ser alterados por meio do arquivo TVT.txt.

Assistente de Transferência de Certificado

O Assistente de Transferência de Certificado do Client Security dá orientação no processo de transferência das chaves privadas associadas aos certificados do CSP (provedor de serviços criptográficos) Microsoft baseado em software para o CSP baseado em hardware do Client Security Solution. Após a transferência, as operações que envolvam os certificados serão mais protegidas porque as chaves privadas serão protegidas pelo chip de segurança integrado.

Reconfiguração da Senha de Hardware

Esta ferramenta cria um ambiente protegido que é executado independentemente do Windows e ajuda a reconfigurar senhas esquecidas de ligação e de unidades de disco rígido. Sua identidade é estabelecida respondendo a um conjunto de perguntas que você criar. É recomendável criar esse ambiente protegido o mais breve possível, antes que uma senha seja esquecida. Não é possível reconfigurar uma senha de hardware esquecida até que esse ambiente protegido seja criado na unidade de disco rígido e após sua inscrição. Essa ferramenta está disponível somente em computadores ThinkCentre e ThinkPad selecionados.

Suporte para Sistemas sem Trusted Platform Module

O Client Security Solution 6.0 agora suporta sistemas das marcas IBM e Lenovo que não tenham um chip de segurança integrado compatível. Isso permitirá uma instalação padrão em toda a empresa para criar um ambiente de segurança homogêneo. Os sistemas que possuem o hardware de segurança integrado serão mais robustos contra ataques; contudo, as máquinas somente com software também se beneficiarão da segurança e funcionalidade adicionais.

System Migration Assistant

O SMA (System Migration Assistant) é uma ferramenta de software que os administradores de sistemas podem utilizar para migrar o ambiente de trabalho de um usuário de um sistema para outro. O ambiente de trabalho de um usuário inclui os seguintes itens:

- Preferências do sistema operacional, tais como configurações do desktop e de conectividade de rede
- Arquivos e pastas
- Configurações customizadas de aplicativos, tais como os favoritos de um navegador da Web ou as preferências de edição no Microsoft Word

- Contas de usuários

Os administradores de sistemas pode utilizar o SMA para configurar um ambiente de trabalho padrão para uma empresa ou para fazer upgrade do computador de um usuário individual. Os usuários individuais podem utilizar o SMA para fazer o backup de um computador ou para migrar configurações e arquivos de um computador para outro. Por exemplo, de um computador desktop para um computador portátil (laptop).

Diferenças de OEM

O Client Security Solution 6.0 não estará disponível para sistemas OEM no momento. O Rescue and Recovery não alavancará nenhum dos aplicativos do Client Security Solution em máquinas OEM.

Capítulo 2. Considerações sobre Instalação

Antes de instalar o ThinkVantage Rescue and Recovery, você deve compreender a arquitetura de todo o aplicativo.

Rescue and Recovery

O Rescue and Recovery tem duas interfaces principais. A interface primária opera no ambiente Windows XP ou Windows 2000. A interface secundária (o ambiente de Pré-desktop do Rescue and Recovery) opera independentemente do sistema operacional Windows XP ou Windows 2000, no ambiente Windows PE.

Notas:

1. O Rescue and Recovery só funcionará com a versão Não-BIOS do Computrace se o Rescue and Recovery for instalado primeiro, e depois o Computrace for instalado. Consulte Capítulo 8, "Boas Práticas", na página 113.
2. Se você tentar instalar o SMS em um sistema com o Rescue and Recovery instalado com a área do Windows PE já instalada como uma partição virtual, o SMS não será instalado. Tanto o Windows PE quanto o SMS utilizam o diretório C:\minint para seu sistema de arquivos. A maneira de instalar ambos ao mesmo tempo é instalar o Rescue and Recovery 2.0 como uma partição Tipo 12. Consulte "Instalando o Rescue and Recovery em uma Partição de Serviço do Tipo 12" na página 126 para obter instruções sobre a instalação do Tipo 12.
3. Um possível risco de segurança pode ser criado quando o Microsoft Recovery Console for instalado em um sistema com o Rescue and Recovery. O Microsoft Recovery Console procura por todas as pastas com o caminho C:*\system32\config\ e, se localizar esse caminho, supões que seja um sistema operacional. Se as entradas do registro que exigem uma senha do Windows não estiverem presentes, o console de recuperação permitirá que um usuário escolha o sistema operacional e, em seguida, obtenha acesso a toda a unidade de disco rígido sem precisar digitar uma senha.

Considerações sobre Instalação sobre outra Versão

O Rescue and Recovery Versão 3.0 suporta uma operação de instalação sobre o Rescue and Recovery 2.0.

Recomenda-se fazer um novo backup após a instalação do Rescue and Recovery 3.0. Isso pode ser feito utilizando um script ou a interface com o usuário.

Estas são as etapas básicas que devem ser seguidas para obter um conjunto completo de backups:

1. Copie os Backups Anteriores para uma unidade de CD/DVD ou uma unidade de disco rígido USB (se desejar).
2. Exclua os backups atuais.
3. Execute um backup básico.

O script a seguir copiará backups para uma unidade de disco rígido USB, excluirá os backups atuais e, em seguida, executará um backup básico.

```
@echo off

::Change directories to \Program Files\IBM\IBM Rescue and Recovery
cd %rr%
```

```
::copy backups to the USB drive
rrcmd copy location=U

::Delete All backups from local HDD silently
rrcmd delete location=L level=0 silent

::Perform a New Base Backup to local HDD silently
rrcmd backup location=L name="Rescue and Recovery 2.0 Base" silent
```

Client Security Solution

Ao implementar o Client Security Solution 6.0, os aspectos a seguir devem ser levados em conta.

O Client Security Solution incluiu no código os drivers e o suporte de software necessários para ativar o software de segurança TPM (Trusted Platform Module) da máquina que irá receber o Client Security Solution 6.0. A ativação do hardware exige pelo menos uma reinicialização, já que o chip é na verdade controlado através do BIOS e exige uma autenticação bem-sucedida do BIOS para concluir o procedimento. Em outras palavras, se uma senha de Administrador/Supervisor do BIOS estiver configurada, ela será exigida para ativar/desativar o Trusted Platform Module.

Antes que seja possível executar qualquer função pelo Trusted Platform Module, o "Direito à Propriedade" deve primeiro ser inicializado. Cada sistema terá um e somente um Administrador do Client Security Solution que irá controlar as opções do Client Security Solution. Esse administrador deverá ter privilégios de administrador do Windows. O administrador pode ser inicializado utilizando scripts de implementação XML.

Depois que o Direito à Propriedade do sistema estiver configurado, cada usuário adicional do Windows que efetuar login no sistema verá automaticamente o Assistente de Configuração de Segurança do Cliente, para poder inscrever-se e inicializar as chaves e credenciais de segurança do cliente.

Emulação de Software para o Trusted Platform Module

O Client Security Solution tem a opção de executar sem um Trusted Platform Module em sistemas qualificados. A funcionalidade será exatamente a mesma, exceto que utilizará chaves baseadas em software em vez de chaves protegidas por hardware. O software também pode ser instalado com uma chave para forçá-lo a utilizar sempre chaves baseadas em software em vez de alavancar o Trusted Platform Module. Essa é uma decisão no momento da instalação e não pode ser revertida sem desinstalar e reinstalalar o software.

A sintaxe para forçar uma emulação de software do Trusted Platform Module é a seguinte:

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

Cenários de Upgrade

Consulte "Cenários de Software Instalado" na página 102 para obter informações sobre como fazer upgrade de níveis anteriores do Client Security Solution.

Capítulo 3. Customização do Rescue and Recovery

Este capítulo fornece informações que podem ser utilizadas para customizar o ThinkVantage Rescue and Recovery.

Produzindo uma Implementação Simples com um Ícone Criar Backup Básico no Desktop

Antes de iniciar este procedimento, assegure-se de que o arquivo ou arquivos TVT, como o z062zaa1025us00.tvt, estejam localizados no mesmo diretório do executável ou do arquivo MSI, ou a instalação falhará. Se o nome do arquivo for setup_tvtrnr3_1027**c**.exe, então você fez download do pacote combinado. Essas instruções são para os arquivos que podem ser transferidos separadamente por download a partir da página de download de *Arquivos de idioma individual de uma Grande Empresa.*

Para executar uma implementação simples que coloque um ícone de backup no desktop do usuário, faça o seguinte:

1. Extraia o SETUP_TVTRNR*XXXX*.EXE (em que *XXXX* é o ID de construção) em um diretório temporário:

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

2. Customize o arquivo TVT.TXT, conforme for necessário. Por exemplo, talvez você queira planejar um backup semanal às terças-feiras, às 15 h. Para isso, inclua as seguintes entradas na seção [Rescue and Recovery] do TVT.TXT. (Consulte o Apêndice B, "Configurações e Valores do TVT.TXT", na página 141 para obter informações adicionais sobre configuração).

   ```
   ScheduleHour=15

   ScheduleMinute=00

   ScheduleDayOfTheWeek=2
   ```

3. Copie também o arquivo Z062ZAA1025US00.TVT para C:\tvtrr. O arquivo TVT deve estar na mesma pasta do arquivo MSI.
4. Inicie a instalação do MSI, adiando a reinicialização:

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

   Nota: O comando acima foi modificado para caber nesta página. Digite esse comando como uma cadeia.
5. Personalize o ambiente do Rescue and Recovery. (Consulte o "Área Pré-desktop" na página 19 para obter informações detalhadas).
6. Exclua os arquivos temporários do diretório C:\TVTRR. (Consulte o "Ambiente Windows" na página 16).
7. Grave um arquivo de comando com os seguintes comandos:

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

   Nota: O comando acima foi modificado para caber nesta página. Digite esse comando como uma cadeia.
8. Crie um atalho em Todos os Usuários do Desktop denominado ″Criar Backup Básico.″ (Especifique seu caminho no campo **Digite o Local** do item).
9. Execute o utilitário Sysprep no sistema.
10. Crie a imagem para implementação.

Depois que o usuário cliente receber a imagem e personalizar o computador, o usuário clica no ícone **Criar Backup Básico** para iniciar o Rescue and Recovery e salvar o backup básico.

Capturando uma Imagem do Sysprep no Backup Básico

Para capturar uma imagem do utilitário Sysprep no backup básico, faça o seguinte:

1. Execute uma instalação administrativa:

```
:: Extract the WWW EXE to the directory C:\IBMRR
     start /WAIT setup_tvtrnrXXXX.exe /a /s /v"/qn TARGETDIR="C:\TVTRR"" /w
```

2. Inclua a seguinte seção no final do arquivo TVT.TXT em C:\TVTRR\Program Files\IBM ThinkVantage\Rescue and Recovery

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

3. Instale o Rescue and Recovery utilizando o arquivo MSIEXE:
   a. Em todos os MSIs, inclua o seguinte código de geração do log de instalação:

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

   b. Para instalar os arquivos de instalação utilizando o arquivo MSIEXE, digite o seguinte comando:

```
: Perform the install of Rescue and Recovery

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

   c. Para instalar silenciosamente os arquivos de instalação utilizando MSIEXE:

   Com reinicialização no final, digite o seguinte comando:

```
: Silent install using the MSI with a reboot
: Type the following command on one line

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

   Com reinicialização suprimida, digite o seguinte comando:

```
: Silent install using the MSI without a reboot
: Type the following command on one line

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

4. Digite os seguintes comandos:

```
:Start the Rescue and Recovery Service
net start  "TVT Backup Service"

:Create Sysprep Base Backup to Local Hard Drive
: Type the following command on one line

cd \"Program Files"\"IBM ThinkVantage\Rescue and Recovery"
rrcmd sysprepbackup location=l name=Sysprep Backup"
```

   Se você deseja utilizar uma senha, inclua a sintaxe `password=`*`pass`*.

5. Execute sua implementação específica do Sysprep quando a seguinte mensagem for exibida:

```
************************************************
** 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. Encerre e reinicialize a máquina quando o Sysprep estiver concluído.

   Nota: O sistema operacional será reinicializado na área Pré-desktop do Rescue and Recovery. Você verá uma barra de status que diz **Restauração do Sistema em Progresso**
7. Quando concluído, você verá uma mensagem que diz **O Backup do Sysprep está Concluído**.
8. Desligue o sistema utilizando o botão liga/desliga.
9. Capture a imagem para implementação.

Capturando uma Máquina de Várias Partições e Excluindo Arquivos de um Backup do Sysprep

Para capturar várias partições em um backup do utilitário Sysprep, faça o seguinte:

1. Execute uma instalação administrativa:

   ```
   :: Extract the WWW EXE to the directory C:\TVTRR
        start /WAIT setup_tvtrrXXXX.exe /a /s /v"/qn TARGETDIR="C:\TVTRR"" /w
   ```

2. Assegure-se ou inclua a seguinte seção no final do arquivo TVT.TXT em C:\\"Program Files"\"IBM ThinkVantage\Rescue and Recovery":\tvtrr\

   ```
   [Backup0]
   BackupVersion=2.0

   [BackupDisk]
   CustomPartitions=0
   ```

   Para EXCLUDE uma partição, inclua o seguinte no arquivo TVT.TXT:

   ```
   [BackupDisk]
   CustomPartitions=1

   [PartitionX].
   IncludeInBackup=0
   ```

   em que **X** é o Número da Partição.
3. Se você deseja excluir os arquivos .MPG e JPG dos backups, inclua-os em IBMFILTER.TXT, como no exemplo a seguir:

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

4. Instale o Rescue and Recovery utilizando MSIEXE:
   a. Em todos os MSIs, inclua o seguinte código de geração do log de instalação:

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

   b. Para instalar os arquivos de instalação utilizando MSIEXE, digite o seguinte comando:

      ```
      : Perform the install of Rescue and Recovery

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

   c. Para instalar silenciosamente os arquivos de instalação utilizando MSIEXE:

      Com reinicialização no final, digite o seguinte comando:

```
: Silent install using the MSI with a reboot

: Type the following command on one line
start /WAIT msiexec /i "C:\TVTRR\Rescue and Recovery - Client
Security Solutiion.msi" /qn
```

Com reinicialização suprimida, digite o seguinte comando:

```
: Silent install using the MSI without a reboot

: Type the following command on one line
start /WAIT msiexec /i "C:\TVTRR\Rescue and Recovery -
Client Security Solutiion.msi" /qn REBOOT="R"
```

5. Digite os seguintes comandos:

```
:Start the Rescue and Recovery Service
net start  "TVT Backup Service"

:Create Sysprep Base Backup to Local Hard Drive

: Type the following command on one line
cd \"Program Files"\IBM ThinkVantage Rescue and Recovery"
rrcmd sysprepbackup location=L name="Sysprep Base Backup"
```

Se você deseja utilizar uma senha, inclua a sintaxe `password=pass`.

6. Execute sua implementação específica do Sysprep quando a seguinte mensagem for exibida:

```
************************************************
** 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. Encerre e reinicialize a máquina quando o Sysprep estiver concluído.

   Nota: O sistema operacional será reinicializado na área Pré-desktop do Rescue and Recovery. Você verá uma barra de status que diz **Restauração do Sistema em Progresso**

8. Quando concluído, você verá uma mensagem que diz **O Backup do Sysprep está Concluído**.
9. Desligue o sistema utilizando o botão liga/desliga.
10. Capture a imagem para implementação.

Ambiente Windows

Incluindo e Excluindo Arquivos em Backups

O Rescue and Recovery possui amplos recursos de inclusão e exclusão. Ele pode incluir e excluir um arquivo ou uma pasta individual ou uma partição inteira.

Os arquivos que controlam as funções de inclusão e exclusão, listados por ordem de precedência, são mostrados a seguir. Todos os arquivos estão localizados no diretório C:\program files\ibm thinkvantage\rescue and recovery.

1. IBMFILTER.TXT
2. GUIEXCLD.TXT

Por padrão, o usuário final pode selecionar arquivos e pastas individuais para serem excluídos do backup. Esses arquivos e pastas são armazenados no arquivo GUIEXCLD.TXT.

Se um administrador deseja garantir que o backup de um determinado arquivo ou pasta seja sempre feito, poderá incluir os nomes ou tipos de arquivos no arquivo IBMIFILTER.TXT. Qualquer entrada desse arquivo será incluída em um backup, independentemente de uma entrada no arquivo GUIEXCLD.TXT.

Os administradores também têm a capacidade de sempre excluir um arquivo, uma pasta ou uma partição de um backup.

Os itens a seguir são sempre excluídos de qualquer backup:
- PAGEFILE.SYS
- HIBERFILE.SYS
- C:\SYSTEM VOLUME INFORMATION

Quando restaurado, o PAGEFILE.SYS e o HIBERFILE.SYS serão restaurados automaticamente pelo Windows. Além disso, os dados da Restauração do Sistema do Windows serão restaurados com um novo ponto de restauração pelo Windows, após a restauração de um backup.

IBMFILTER.TXT

O formato do arquivo é:

- Uma linha por entrada de regra de inclusão/exclusão.
- Se mais de uma regra se aplicar a um arquivo ou pasta, a regra mais recente se aplicará. As entradas da parte inferior do arquivo terão precedência.
- As entradas devem começar com:
  - **;**

    para um comentário
  - **I**

    deve incluir arquivos ou pastas que coincidem com a entrada
  - **X**

    deve excluir arquivos ou pastas que coincidem com a entrada
  - **S**

    devem incluir Armazenamento de uma Única Instância em um arquivo ou uma pasta
  - **i**

    para arquivos ou pastas que você pode optar por incluir
  - **x**

    para arquivos ou pastas que você pode optar por excluir
  - **s**

    opcionalmente utilizado para identificar um arquivo ou pasta como Armazenamento de uma Única Instância que normalmente seria incluída.

```
 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=?:\Arquivos de programas\*
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
```

Customizando Outros Aspectos do Rescue and Recovery

Você pode customizar vários aspectos do Rescue and Recovery utilizando um arquivo externo chamado TVT.TXT que é definido antes do processo de instalação. O arquivo TVT.TXT está localizado no subdiretório C:\Program Files\IBM ThinkVantage\.

O arquivo TVT.TXT seguirá o formato padrão do arquivo INI do Windows com os dados organizados por seções entre [] e uma entrada por linha deste formato:

`setting=`*`value`*

Por exemplo, se você não deseja criptografar todos os dados de backup, inclua as seguintes linhas no arquivo TVT.TXT:

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

O parâmetro `0` após o EncryptBackupData conduz o Rescue and Recovery a não criptografar o backup.

Uma lista completa de cadeias, parâmetros e definições padrão de configuração da seção [Rescue and Recovery] do TVT.TXT são apresentadas no Apêndice B, “Configurações e Valores do TVT.TXT”, na página 141.

Registro de Problema

No momento, não há como transmitir automaticamente por meio de FTP ou e-mail a partir do ambiente do Rescue and Recovery; o usuário final deverá utilizar o e-mail integrado ao navegador, bem como o local dos arquivos para transmitir. A transferência de dados dinâmicos não é suportada, mas a função de log compactará os eventos de log em um arquivo e conduzirá o usuário do local e do nome do arquivo de compactação que puder ser enviado por e-mail. Isso criará o arquivo XML do *Registro de Problema da Req 115*, que combina todas as informações exibidas em Informações Sobre o Sistema (informações Current HW, eGatherer e de log de diagnóstico do PCDR), que serão colocadas em um local que pode ser facilmente localizado e acessível a partir do ambiente do Rescue and Recovery e do S.O. – C:\IBMSHARE.

Diagnósticos: é um aplicativo básico disponível na Área Pré-desktop que ajuda na determinação do problema. A saída desses testes será armazenada de modo que possa ser visualizada ou transmitida a um help-desk. O Rescue and Recovery fornecerá ferramentas para a recuperação de uma versão de backup anterior do ambiente Windows do usuário.

O Rescue and Recovery conterá ferramentas para fazer uma restauração completa de uma partição do usuário para uma versão anterior, bem como as ferramentas para recuperar arquivos individuais. As ferramentas fornecerão acesso a um backup de dados do usuário. A capacidade de recuperar todos ou alguns desses dados será fornecida por essas ferramentas.

OSFILTER.TXT

Esse arquivo recupera o sistema operacional do usuário e os aplicativos, sem impacto para os dados. O Rescue and Recovery fornece a capacidade de restaurar de forma seletiva determinados arquivos e pastas (incluindo subpastas) utilizando enumeração explícita e filtragem curinga sem excluir quaisquer outros dados. Um arquivo externo definirá quais arquivos, pastas ou tipos de arquivos (alavancando curingas) incluem S.O. e Aplicativos. Esse arquivo pode ser personalizado pelo administrador e um arquivo externo padrão será fornecido. Quando o usuário optar por recuperar o sistema operacional, verá um menu que permite selecionar Apenas Restaurar com as seguintes opções do Windows: Apenas os arquivos que atendem as regras contidas neste arquivo externo serão restaurados. O administrador pode personalizar o conteúdo desse arquivo externo.

Para visualizar o arquivo OSFILTER.TXT, utilize este caminho: `cd %RR%`. Consulte “IBMFILTER.TXT” na página 17 para obter informações sobre o formato de arquivo.

Área Pré-desktop

Para customizar partes da Área Pré-desktop do Rescue and Recovery, que são iniciadas mesmo se o sistema operacional não abrir, use o programa utilitário RRUTIL.exe para OBTER (GET) e COLOCAR (PUT) arquivos. Esses arquivos e suas opções de personalização estão listadas na tabela a seguir:

Tabela 1. Arquivos RRUTIL.exe e Opções de Customização

Arquivo / Diretório	Opções de Personalização
\MININT\SYSTEM32 WINBOM.INI	Incluir um endereço IP estático, alterar a resolução de vídeo

Tabela 1. Arquivos RRUTIL.exe e Opções de Customização (continuação)

Arquivo / Diretório	Opções de Personalização
\MININT\INF \MININT\SYSTEM32\DRIVERS	Incluir drivers de dispositivo
MAINBK.BMP	Modificar o segundo plano do ambiente
MINIMAL_TOOLBAR(1).INI	Desativar a barra de endereços
NORM1.INI	Configurar o navegador Opera, desativar a barra de endereços do Opera, alterar as configurações de proxy do Opera, especificar diretório fixo de download, incluir extensão de arquivo específica para lista de arquivos transferidos por download, alterar o comportamento dos arquivos com extensões específicas
OPERA_010.CMD	Excluir os favoritos dos usuários da janela
OPERA6.INI	Configurar o navegador do Opera, desativar a barra de endereços
PEACCESS*xx*.INI (em que *xx* é a designação de idioma)	Ambiente de pré-inicialização: fontes da GUI principal, segundo plano do ambiente, entradas e funções do painel esquerdo e direito, sistema de ajuda baseado em HTML
STANDARD_MENU.INI	Ativar a exibição da janela "Salvar como"

Utilizando o RRUTIL.EXE

Você pode obter o RRUTIL.EXE e outros utilitário mencionados neste guia no Web site que contém este documento.

O procedimento a seguir lista as etapas para OBTER arquivos do ambiente do Rescue and Recovery e COLOCAR arquivos nele. Esses procedimentos são utilizados para todas as personalizações de arquivos do ambiente do Rescue and Recovery.

Para utilizar o RRUTIL.EXE, faça o seguinte:

1. Copie o RRUTIL.exe na raiz da unidade C.
2. Crie o arquivo GETLIST.TXT com a seguinte sintaxe:

   `\preboot\usrintfc\`*`nome do arquivo`*

   Salve o arquivo como C:\TEMP\GETLIST.TXT.
3. No prompt de comandos, digite o comando RRUTIL.exe e um dos comutadores definidos na tabela a seguir. Em seguida, conclua o comando com os parâmetros apropriados, conforme mostrado na tabela a seguir.

Tabela 2. Opções de Comando e de Comutador

Opções de Comando e de Comutador	Resultado
`RRUTIL -l1`	Lista o conteúdo do diretório de pré-inicialização
`RRUTIL -l2`	Lista o conteúdo do diretório minint
`RRUTIL -l4`	Lista o conteúdo da raiz da unidade C ou da raiz da partição tipo 12
`RRUTIL -g C:\temp\getlist.txt C:\temp`	Obtém arquivos da partição de pré-inicialização

Tabela 2. Opções de Comando e de Comutador (continuação)

Opções de Comando e de Comutador	Resultado
`RRUTIL -d C:\temp\ dellist.txt`	Exclui arquivos da partição de pré-inicialização.
`RRUTIL -p C:\temp`	Inclui ou substitui arquivos da partição de pré-inicialização.
`RRUTIL -r path \oldname.ext newname.ext` `RRUTIL -r \temp\rr\test.txt test2.txt` o arquivo está no diretório preboot\rr	Renomeia um arquivo na Área Pré-desktop.
`RRUTIL -bp C:\temp`	Atualiza ou substitui arquivos da partição virtual RRBACKUPS.

`RRUTIL -bl path`
 	
RRUTIL -bl lista em `C:\rr-list.txt`
 	
`rrutil -bl c:\rrtemp`
	Lista o diretório RRBACKUPS

`RRUTIL -br RRbackups\C\n` em que n é o número do backup	Exclui o conteúdo do backup.
`RRUTIL -bg C:\temp\bgetlist.txt C:\temp`	Copia arquivos individuais do \RRBACKUPS.
`RRUTIL -s`	Espaço consumido pelo RRBACKUPS.

4. Depois de executar a rotina GET, você pode então editar o arquivo utilizando um editor de texto padrão.

Exemplo: PEACCESSIBMxx.INI

Este exemplo refere-se ao PEACCESSIBM*xx*.INI, que é um arquivo de configuração em que você pode personalizar elementos do ambiente do Rescue and Recovery (consulte "Personalizando o Ambiente de Pré-inicialização" na página 22).

Nota: *xx* no nome do arquivo representa uma das seguintes abreviações de idioma em duas letras:

Tabela 3. Códigos do Idioma

Código do Idioma em Duas Letras	Idioma
br	Português do Brasil
dk	Dinamarquês
en	Inglês
fi	Finlandês
fr	Francês
gr	Alemão
it	Italiano
jp	Japonês
kr	Coreano
nl	Holandês
não	Norueguês
po	Português
sc	Chinês Simplificado
sp	Espanhol
sv	Sueco
tc	Chinês Tradicional

Obtendo o arquivo PEACCESSIBMEN.INI do ambiente do Rescue and Recovery:

1. Crie o arquivo GETLIST.TXT com os seguintes parâmetros:

   ```
   \preboot\reboot\usrintfc\PEAccessIBMen.ini
   ```
2. Salve o arquivo como C:\TEMP\GETLIST.TXT.
3. No prompt de comandos, digite o seguinte comando:

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

Colocando o arquivo PEACCESSIBMEN.INI novamente no ambiente do Rescue and Recovery. Em uma linha de comandos, emita o seguinte comando:

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

Nota: A rotina PUT (**-p**) utiliza a estrutura de diretórios criada na rotina GET (**-g**). Para a colocação correta do arquivo editado, assegure-se de que o arquivo editado esteja localizado no mesmo diretório especificado no arquivo GETLIST.TXT, como no exemplo a seguir:

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

Exemplo: Incluindo Drivers de Dispositivo na Área Pré-desktop

1. Obtenha drivers de dispositivo do Web site ou de outra mídia do fornecedor.
2. Crie as seguintes estruturas de diretório:

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

   ```
   C:\TEMP\MININT\SYSTEM32\DRIVERS
   ```
3. Copie todos os arquivos *.INF do driver de rede para o diretório MININT\INF. (Por exemplo, E100B325.INF deve estar no diretório \MININT\INF).
4. Copie todos os arquivos *.SYS para o diretório \MININT\SYSTEM32\DRIVERS. (Por exemplo, E100B325.SYS deve estar no diretório MININT\SYSTEM32\DRIVERS).
5. Copie todos os arquivos *.DLL, *.EXE ou outros arquivos relacionados para o diretório \MININT\SYSTEM32\DRIVERS. (Por exemplo, os arquivos E100B325.DIN ou INTELNIC.DLL devem estar no diretório MININT\SYSTEM32\DRIVERS).

   Notas:
   a. Os arquivos do catálogo são desnecessários, uma vez que não são processados pelo ambiente do Rescue and Recovery. As instruções anteriores aplicam-se a qualquer driver de dispositivo que possa ser necessário para configurar o computador.
   b. Devido à limitação do Windows Professional Edition, talvez seja necessário aplicar manualmente alguns aplicativos ou definições de configuração, como atualizações de registro.
6. Para colocar os drivers de dispositivo no ambiente do Rescue and Recovery, digite o seguinte em uma linha de comandos:

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

Personalizando o Ambiente de Pré-inicialização

Editando o arquivo de configuração PEACCESSIBM*xx*.INI (em que *xx* é a designação do idioma), você pode customizar os seguintes elementos do ambiente do Rescue and Recovery:

- As fontes da GUI principal
- O segundo plano do ambiente
- As entradas e funções no painel esquerdo da interface com o usuário
- O sistema de ajuda baseado em HTML do ambiente do Rescue and Recovery

Nota: Para obter, editar e substituir o arquivo PEACCESSIBMEN.INI, consulte “Exemplo: PEACCESSIBMxx.INI” na página 21.

Alterando a Fonte da GUI Principal

Você pode alterar a fonte da GUI (Interface Gráfica com o Usuário) principal. Talvez as configurações padrão não exibam todos os caracteres corretamente, dependendo do idioma e dos caracteres necessários. No PEACCESSIBM*xx*.INI (em que *xx* é a designação do idioma) a seção [Fonts] contém as configurações padrão do estilo de caractere exibido. A seguir estão as configurações padrão da maioria dos idiomas de conjuntos de caracteres de byte simples:

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

Dependendo de suas necessidades visuais e dos conjuntos de caracteres, as seguintes fontes são compatíveis com o ambiente do Rescue and Recovery. Outras fontes podem ser compatíveis, mas ainda não foram testadas:

- Courier
- Times New Roman
- Comic Sans MS

Alterando o Segundo Plano do Ambiente

O segundo plano do painel direito é um bitmap, MAINBK.BMP, que está localizado no diretório \PREBOOT\USRINTFC. Se você criar sua própria imagem de bitmap para o segundo plano do painel direito, ela deverá estar em conformidade com as seguintes dimensões:

- 620 pixels de largura
- 506 pixels de profundidade

Você deve colocar o arquivo no diretório \PREBOOT\USRINTFC para que o Rescue and Recovery esteja presente no segundo plano desejado.

Nota: Para obter, editar e substituir o arquivo MAINBK.BMP, consulte “Utilizando o RRUTIL.EXE” na página 20.

Alterando Entradas e Funções do Painel Esquerdo

A alteração das entradas do painel esquerdo requer a edição do arquivo PEACCESSIBM*xx*.INI (em que *xx* é a designação do idioma). Para obter informações sobre como obter o PEACCESSIBM*xx*.INI a partir do ambiente do Rescue and Recovery e como substituir o arquivo, consulte “Utilizando o RRUTIL.EXE” na página 20.

O Rescue and Recovery tem vinte e uma entradas no painel esquerdo. Embora as funções sejam diferentes, todas as entradas têm os mesmos elementos básicos. A seguir está um exemplo de uma entrada do painel esquerdo:

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

Tabela 4. Entradas do Painel à Esquerda e Opções de Customização

Entrada	Opções de Customização
00-01	Totalmente customizável.
02	Deve permanecer um botão tipo 1 (consulte a Tabela 5 na página 24). O texto pode ser alterado. Uma função do aplicativo ou de ajuda pode ser definida. Nenhum ícone pode ser incluído.
03-06	Totalmente customizável.

Tabela 4. Entradas do Painel à Esquerda e Opções de Customização (continuação)

Entrada	Opções de Customização
07	Deve permanecer um tipo 1. O texto pode ser alterado. Uma função do aplicativo ou de ajuda pode ser definida. Nenhum ícone pode ser incluído.
08-10	Totalmente customizável.
11	Deve permanecer um botão tipo 1. O texto pode ser alterado. Uma função do aplicativo ou de ajuda pode ser definida. Nenhum ícone pode ser incluído.
16	Deve permanecer um tipo 1. O texto pode ser alterado. Uma função do aplicativo ou de ajuda pode ser definida. Nenhum ícone pode ser incluído.
17–22	Totalmente customizável.

Definindo Tipos de Entrada: **Button00** deve ser um identificador exclusivo. O número determina a ordem na qual os botões são exibidos no painel esquerdo.

Button00=[0-8] Esse parâmetro determina o tipo de botão. Esse número pode ser um inteiro de 0 a 8. A tabela a seguir explica o tipo e o funcionamento de cada tipo de botão:

Tabela 5. Parâmetros de Tipo de Entrada

Parâmetro	Tipo de Botão
0	Esvaziar campo. Utilize esse valor quando desejar deixar uma coluna em branco ou sem uso.
1	Texto do título da seção. Utilize essa configuração para estabelecer um agrupamento principal ou um título de seção.
2	Ativação do aplicativo. Defina um aplicativo ou um arquivo de comando para ser iniciado quando o usuário clicar no botão ou no texto.
3	Ajuda do Opera do ambiente do Rescue and Recovery. Defina um tópico de ajuda para ser ativado com o navegador Opera.
4	Exibir uma janela de mensagens de reinicialização antes da ativação. Utilize esses valores para determinar que a GUI apresente uma mensagem ao usuário de que o computador deverá ser reiniciado para que a função especificada seja executada.
5	Reservado para Lenovo Group Ltd.
6	Reservado para Lenovo Group Ltd.
7	Ativar e esperar. Os campos que seguem essa especificação forçam o ambiente a aguardar um código de retorno do aplicativo ativado antes de prosseguir. Espera-se que o código de retorno esteja na variável de ambiente, %errorlevel%.
8	Ativar aplicativo. A GUI recupera o Código do País e o idioma antes de iniciar o aplicativo. É utilizado em links da Web que tenham scripts CGI para abrir uma página da Web de um determinado país ou de um idioma específico.
9	Reservado para Lenovo Group Ltd.
10	Reservado para Lenovo Group Ltd.

Definindo Campos de Entrada:

Button00=[0-10], "title"
O texto após o parâmetro de tipo de botão especifica o texto ou o título do botão. Se o texto exceder a largura do painel esquerdo, ele será recortado e as reticências indicarão que existem mais caracteres a seguir. O texto completo do título é exibido ao utilizar a ajuda instantânea.

Button00=[0-10], "title", file.bmp
Após o texto do título, especifique o nome do arquivo do bitmap que você deseja utilizar como um ícone para o botão que está sendo criado. O bitmap não pode exceder 15 pixels por 15 pixels para se ajustar corretamente.

Button00=[0-10], "title", file.bmp, [0 ou 1]
Essa configuração controla o ambiente para exibir ou ocultar a entrada. O valor `0` oculta a entrada. Se o valor for definido como `0`, então uma linha em branco será exibida. O valor 1 exibe o valor.

Button00=[0-10], "title", file.bmp, [0 ou 1], 1
Essa é uma função reservada e deve ser sempre definida como 1.

Button00=[0-10], "title", file.bmp, [0 ou 1], 1, [0 ou 1]
Para solicitar uma senha antes de iniciar um aplicativo, coloque um valor de 1 nessa posição. Se você definir esse valor como `0`, nenhuma senha será exigida antes de o aplicativo especificado ser iniciado.

Button00=[0-10], "title", file.bmp, [0 ou 1], 1, [0 ou 1], %sysdrive%[pathname\executable]
O valor de `%sysdrive@` deve ser a letra da unidade de inicialização. Depois da letra da unidade de inicialização, você deve fornecer um caminho completo para um arquivo do aplicativo ou de comandos.

Button00=[0-10], "title", file.bmp, [0 ou 1], 1, [0 ou 1],%sysdrive%[pathname\executable], [parameters]
Fornece qualquer número de parâmetros exigido pelo aplicativo de destino que está sendo iniciado.

Se você não estiver fornecendo valores para vários campos, deverá fornecer as vírgulas necessárias para que a definição do botão seja aceita e executada corretamente. Por exemplo, se você estiver criando um título para o grupo, ″Rescue and Recover,″ o código da entrada seria o seguinte:

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

As entradas 02, 07, 11 e 16 devem permanecer entradas do tipo `0` (ou título) e elas sempre caem em seus locais numéricos. A disponibilidade das entradas que caem nos títulos pode ser reduzida definindo-se entradas totalmente personalizáveis do tipo 0-linhas em branco no painel esquerdo. Entretanto, o número total de entradas não pode exceder vinte e três.

A tabela a seguir mostra a função e os executáveis que você pode iniciar a partir das entradas do painel esquerdo:

Tabela 6. Funções e Executáveis do Painel Esquerdo

Função	Executável
Recuperar arquivos	WIZRR.EXE
Restaurar a partir de um backup	WIZRR.EXE
Criar arquivo de migração	WIZRR.EXE
Abrir navegador	OPERA.EXE

Tabela 6. Funções e Executáveis do Painel Esquerdo (continuação)

Função	Executável
Mapear uma unidade de rede	MAPDRV.EXE
Diagnosticar hardware	RDIAGS.CMD; ativa o aplicativo PC Dr, apenas para modelos de pré-instalação da IBM e Lenovo
Criar disquetes de diagnóstico	DDIAGS.CMD

Alterando Entradas e Funções do Painel Direito

A alteração das entradas do painel direito requer a edição do arquivo PEACCESSIBM*xx*.INI (em que *xx* é a designação do idioma). Para obter informações sobre como obter o PEACCESSIBM*xx*.INI do ambiente do Rescue and Recovery e como substituir o arquivo, consulte "Exemplo: PEACCESSIBMxx.INI" na página 21.

Os links de função, as mensagens do usuário e o status da janela do painel direito são personalizáveis.

Personalizando os Links de Função do Painel Direito: Para alterar as funções dos links existentes na parte superior do painel direito, modifique a seção [TitleBar] do PEACCESSIBM*xx*.INI (em que *xx* é a designação do idioma). Esses links funcionam da mesma maneira que as entradas do painel esquerdo. Os valores de números do botão vão de 00 a 04. Os mesmos aplicativos que podem ser iniciados a partir do painel esquerdo, podem ser iniciados a partir das entradas [TitleBar]. Consulte "Utilizando o RRUTIL.EXE" na página 20 para obter uma lista completa dos executáveis que podem ser iniciados a partir da barra de título.

Modificando Mensagens do Usuário e Status da Janela: PEACCESSIBM*xx*.INI (em que *xx* é a designação do idioma) contém duas seções com mensagens para o usuário que você pode modificar:

```
[janela Welcome]
[Mensagens de reinicialização]
```

A janela Boas-vindas é definida na seção [Welcome] do PEACCESSIBM*xx*.INI (em que *xx* é a designação do idioma). Dependendo das alterações feitas no painel esquerdo, você poderá alterar as informações na linha de título e nas linhas de 01 a 12. Você pode definir a fonte em que o título, cabeçalho e negrito, será exibido:

```
[Welcome]
Title = "Welcome to Rescue and Recovery"
Line01 = "The Rescue and Recovery(TM) workspace provides a number of tools
to help you recover from problems that prevent you from accessing the Windows(R)
environment."
Line02 = "You can do the following:"
Line03 = "*Rescue and restore your files, folder or backups using Rescue and
Recovery(TM)"
Line04 = "your files, folders or backups using Rescue and Recovery(TM)"
Line05 = "*Configure your system settings and passwords"
Line06 = "your system settings and passwords"
Line07 = "*Communicate using the Internet and link to the Lenovo support site"
Line08 = "use the Internet and link to the IBM support site"
Line09 = "*Troubleshoot problems using diagnostics"
Line10 = "diagnose problems using diagnostics"
Line11 = "Features may vary based on installation options.
For additional information, click Introduction
in the Rescue and Recovery menu."
Line12 = "NOTICE:"
Line13 = "By using this software, you are bound by the
```

```
terms of the License Agreement. To view the license,
click Help in the Rescue and Recovery toolbar,
and then click View License."
Continue = "Continue"
NowShow = "Do not show again"
NoShowCk =0
WelcomeTitle = "Arial Bold"
WelcomeText = "Arial"
WelcomeBold = "Arial Bold"
```

As seguintes configurações são para as funções de Ajuda da Barra de Título da interface com o usuário:

Command0
Uma página HTML para ser iniciada na página de ajuda básica

Command1
Página HTML do Contrato de Licença da Lenovo

HELP Ajuda

LICENSE
Licença

CANCEL
Cancelar

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

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

Para ocultar completamente a janela Boas-vindas, altere `NoShowCk=0` para `NoShowCk=1`. Para alterar as fontes de exibição do título e do texto de boas-vindas, edite as últimas três linhas da seção, de acordo com suas preferências de design.

Nota: Não altere ou exclua as linhas 13 e 14.

Na seção [REBOOT] do arquivo PEACCESSIBM*xx*.INI (em que *xx* é a designação do idioma), você pode modificar os valores das seguintes linhas:

```
NoShowChk=
RebootText=
```

Os dois valores de ″NoShowChk″ são `0` e `1`. A mensagem pode ser ocultada quando o usuário desejar. Quando um usuário clicar na caixa de opções, no momento da exibição da mensagem, o valor será definido como `0`. Para que a mensagem seja exibida, altere o valor para `1`. Se for necessário, a fonte das mensagens na seção [REBOOT] poderá ser alterada. Por exemplo, esse valor poderá ser definido da seguinte maneira:

```
RebootText = "Arial"
```

Nota: As seções a seguir do PEACCESSIBM*xx*.INI (em que *xx* é a designação do idioma) estão disponíveis no arquivo, mas não são personalizáveis: [Messages], [EXITMSG] e [HelpDlg].

Configurando o Navegador Opera

O navegador Opera tem dois arquivos de configuração e um deles contém a configuração padrão. O outro é a configuração ″ativa″. Um usuário final pode fazer alterações à configuração ativa, mas essas alterações serão perdidas quando o Rescue and Recovery for reiniciado.

Para tornar as alterações permanentes no navegador, edite as cópias dos arquivos OPERA6.INI e NORM1.INI que estão no %systemdrive%, C, no seguinte caminho de pasta: C:\PREBOOT\OPERA\PROFILE. A cópia temporária, ″ativa″ do OPERA6.INI está na ramdrive (Z:), no diretório Z:\PREBOOT\OPERA\PROFILE.

Notas:

1. Para obter, editar e colocar os arquivos OPERA6.INI e NORM1.INI, consulte “Utilizando o RRUTIL.EXE” na página 20.
2. O espaço de trabalho do Opera foi modificado para fornecer segurança aprimorada. Como resultado, algumas funções do navegador foram excluídas.

E-mail

O Rescue and Recovery fornece suporte para e-mail baseado na Web por meio do navegador Opera. O Opera fornece e-mail baseado no IMAP que pode ser ativado por meio de uma ampla configuração corporativa, mas não é suportado. Para obter as informações de referência sobre como ativar, leia o Guia do Administrador do Sistema, no endereço:

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

Desativando a Barra de Endereços

Para desativar a barra de endereços no Opera, conclua o seguinte procedimento:

1. Obtenha o arquivo MINIMAL_TOOLBAR(1).INI no C:\PREBOOT\OPERA\PROFILE\TOOLBAR utilizando o processo RRUTIL, descrito em “Utilizando o RRUTIL.EXE” na página 20.
2. Abra o arquivo para edição.
3. Localize a seção [Document Toolbar] do arquivo.
4. Localize a entrada ″Address0″.
5. Coloque um ponto-e-vírgula (; - um delimitador de comentário) na frente da entrada ″Address0″.

   Nota: Parar aqui e continuar na etapa 7 desativa a barra de ferramentas do Opera, mas deixa um botão Ir e o gráfico da barra de ferramentas não-funcionais. Para remover o botão Ir e a barra de ferramentas, continue na etapa 6.
6. Localize as seguintes entradas e, em seguida, coloque um ponto-e-vírgula em frente a cada:

   ```
   Button1, 21197=Go Zoom2
   ```
7. Salve o arquivo.
8. Coloque o arquivo utilizando o processo RRUTIL, conforme descrito em “Utilizando o RRUTIL.EXE” na página 20. A barra de endereços será desativada quando o Opera for executado.

Personalizando Marcadores

O navegador Opera está configurado para ler os marcadores estabelecidos neste arquivo ramdrive: Z:\OPERADEF6.ADR. Esse arquivo é gerado quando o Rescue and Recovery é iniciado a partir do código na rotina de inicialização. A rotina de inicialização importa automaticamente os marcadores do Windows Internet Explorer e inclui alguns marcadores adicionais. Como o arquivo ramdrive, que é

gerado na inicialização é inconstante, inclua os marcadores no Internet Explorer, que é importado automaticamente quando o ambiente do Rescue and Recovery é iniciado.

Você pode excluir alguns ou todos os favoritos do Internet Explorer. Para excluir favoritos específicos de usuários do Windows, faça o seguinte:
1. Obtenha C:\PREBOOT\STARTUP\OPERA_010.CMD utilizando o processo RRUTIL, descrito em "Utilizando o RRUTIL.EXE" na página 20.
2. Abra o arquivo para edição.
3. Localize a seguinte linha no arquivo CMD: PYTHON.EXE.FAVS.PYC Z:\OPERADEF6.ADR.
4. No final dessa linha de tipo de código, digite entre aspas os nomes dos usuários do Windows cujos favoritos você deseja excluir. Por exemplo, se você deseja excluir os favoritos de Todos os Usuários e do Administrador, a linha de código será lida da seguinte maneira:

   ```
   python.exe favs.pyc z:\Operadef6.adr "All Users, Administrator"
   ```
5. Salve o arquivo.
6. Coloque o arquivo utilizando o processo RRUTIL, descrito em "Utilizando o RRUTIL.EXE" na página 20.

Se você não deseja que nenhum dos favoritos do Internet Explorer seja exibido no navegador fornecido no ambiente do Rescue and Recovery, faça o seguinte:
1. Obtenha o C:\PREBOOT\STARTUP\OPERA_010.CMD para edição utilizando o processo RRUTIL, conforme descrito em "Utilizando o RRUTIL.EXE" na página 20.
2. Localize a seguinte linha no arquivo CMD: PYTHON.EXE.FAVS.PYC Z:\OPERADEF6.ADR.
3. Execute uma das seguintes ações:
   a. Digite REM no começo da linha, como a seguir:

      ```
      REM python.exe favs.pyc z:\Operadef6.adr
      ```
   b. Exclua a linha de código do arquivo.
4. Salve o arquivo.
5. Coloque o arquivo novamente utilizando o processo RRUTIL, descrito em "Utilizando o RRUTIL.EXE" na página 20.

Alterando as Configurações do Proxy

Para alterar as configurações do proxy do navegador Opera, faça o seguinte:
1. Obtenha o arquivo C:\PREBOOT\OPERA\PROFILE\NORM1.INI para edição utilizando o processo RRUTIL, descrito em "Utilizando o RRUTIL.EXE" na página 20.
2. Inclua a seção a seguir na parte inferior do arquivo NORM1.INI:

   Nota: A variável [0 ou 1] indica que o item de verificação está ativado (1) ou desativado (0).

   ```
   [Proxy]
   Use HTTPS=[0 or 1]
   Use FTP=[0 or 1]
   Use GOPHER=[0 or 1]
   Use WAIS=[0 or 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 or 1]
   ```

```
Use HTTP=[0 or 1]
Use Automatic Proxy Configuration= [0 or 1]
Automatic Proxy Configuration URL= [URL]

No Proxy Servers Check= [0 or 1]

No Proxy Servers =<IP addresses>
```

3. Salve o arquivo.
4. Coloque o arquivo novamente utilizando o processo RRUTIL, descrito em "Utilizando o RRUTIL.EXE" na página 20.

Para incluir um proxy HTTP, HTTPS, FTP, Gopher ou WAIS, digite `=<address of proxy>` depois da linha apropriada. Por exemplo, se o endereço do seu servidor proxy for http://www.your company.com/proxy, a linha do Servidor HTTP seria lida como a seguir:

```
HTTP Server=http://www.your company.com/proxy
```

Para incluir a porta na entrada, coloque um ponto-e-vírgula depois do endereço e digite o número da porta. O mesmo é verdadeiro para os campos ″Sem Servidores Proxy″ e ″URL de Configuração Automática de Proxy″.

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

Ativando ou Especificando o Caminho Completo de Download

Há várias configurações que você pode definir para ativar a exibição da janela ″Salvar como″. O método mais direto é o seguinte:

1. Obtenha o arquivo C:\PREBOOT\OPERA\DEFAULTS\STANDARD_MENU.INI, utilizando o processo RRUTIL, descrito em "Utilizando o RRUTIL.EXE" na página 20.
2. Na seção `[Link Popup Menu]`, localize esta cadeia:

   ```
   ;;Item, 50761
   ```

3. Remova os dois pontos-e-vírgula e, em seguida, salve o arquivo. Quando o Rescue and Recovery for fechado e reaberto, um usuário final poderá clicar com o botão direito do mouse em um link e a opção ″Salvar Destino como″ será exibida. Isso resulta na exibição da janela ″Salvar como″.

   Nota: Os links diretos (não os links redirecionados) funcionam com o procedimento anterior. Por exemplo, se um link tiver como destino um script .PHP, o Opera salvará apenas o script, não o arquivo para o qual o script aponta.
4. Coloque o arquivo novamente na estrutura de diretórios utilizando o processo RRUTIL, descrito em "Utilizando o RRUTIL.EXE" na página 20.

Para especificar um diretório fixo de download, faça o seguinte:

1. Obtenha o arquivo C:\PREBOOT\OPERA\NORM1.INI utilizando o processo RRUTIL definido, descrito em "Utilizando o RRUTIL.EXE" na página 20.
2. No arquivo, localize esta linha:

   ```
   Download Directory=%OpShare%
   ```

3. Altere `%OpShare%` para o caminho completo do diretório em que você deseja salvar os arquivos transferidos por download.
4. Salve o arquivo NORM1.INI. Quando o Rescue and Recovery for fechado e reaberto, o Opera salvará os arquivos transferidos por download no diretório especificado.
5. Coloque o arquivo novamente utilizando o processo RRUTIL, descrito em "Utilizando o RRUTIL.EXE" na página 20.

Notas:

1. A customização do caminho completo para download não permite que os usuários salvem o arquivo de destino, mesmo se o link for redirecionado.

2. O navegador Opera está configurado para fazer download apenas dos tipos de arquivos .ZIP, .EXE e .TXT, e alterações apenas no comportamento do Opera desses tipos de arquivos. (Existem possivelmente milhares de tipos de arquivos que utilizam uma extensão de arquivo de três letras. Da mesma forma que o ambiente do Rescue and Recovery não tem a intenção de ser um substituto do ambiente Windows, o navegador Opera não tem a intenção de substituir um navegador de serviço completo. O acesso à Internet é fornecido para ajudar os usuários a se familiarizar e a executar. O número de tipos de arquivos reconhecidos é necessariamente limitado. Para fins de resgate e recuperação, os arquivos .ZIP, .EXE e .TXT devem ser suficientes. Se outro tipo de arquivo precisar ser transferido, melhores resultados serão conseguidos pela criação de um arquivo .ZIP, que poderá ser extraído).
3. Os tipos de arquivos são reconhecidos pelo tipo mime em vez de pela extensão do arquivo. Por exemplo, se um arquivo .TXT for denominado com a extensão .EUY, o arquivo continuará aberto no navegador Opera como um arquivo de texto.

Incluindo uma Extensão de Arquivo Específica na Lista de Arquivos Transferidos por Download

Você pode incluir na lista de arquivos que podem ser transferidos por download por meio do navegador do Rescue and Recovery. Para incluir na lista, conclua o seguinte procedimento:

1. Assegure-se de que o Opera esteja fechado e que todas as janelas do Opera estejam fechadas, incluindo os arquivos de ajuda do Rescue and Recovery.
2. Obtenha o arquivo C:\PREBOOT\OPERA\NORM1.INI utilizando o processo RRUTIL, descrito em "Utilizando o RRUTIL.EXE" na página 20.
3. Localize a seção `[File Types]` do arquivo.
4. Utilize a função de procura para descobrir se a extensão do arquivo desejada está listada, mas não funciona; em seguida, execute um dos seguintes procedimentos:
   - Se a extensão for localizada, mas os arquivos com essa extensão não funcionarem corretamente, conclua as seguintes etapas:
     a. Altere o valor após a extensão de 8 para 1. (Um valor de 8 diz ao navegador para ignorar o arquivo. Um valor de 1 instrui o navegador a salvar o arquivo). Por exemplo, altere o seguinte:

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

        a

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

     b. Vá para a seção [File Types Extension] do arquivo NORM1.INI e, em seguida, procure pelo tipo mime do arquivo. Por exemplo, localize o seguinte: VIDEO/MPEG=,8
     c. Altere o valor ,8 para o seguinte:

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

        Nota: Se o valor já definido estiver especificado, não o altere.
     d. Salve o arquivo e, em seguida, copie-o em OPERA6.INI e reinicie o Rescue and Recovery para que as alterações sejam efetivadas.
   - Se a extensão não estiver presente e os arquivos do tipo desejado não funcionarem corretamente, faça o seguinte:
     a. Na seção [File Types Extension] do NORM1.INI, localize a entrada mime temporária. Segue um exemplo:
        temporary=1,,,,lwp,prz,mwp,mas,smc,dgm,|

b. Inclua a extensão do tipo de arquivo na lista. Por exemplo, se você deseja incluir .CAB como uma extensão reconhecida, inclua-a de acordo com a seguinte entrada de amostra:

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

Nota: A vírgula final e o símbolo pipe (|) são essenciais para que essa configuração funcione. Se um deles for omitido, todas as extensões de arquivo da lista poderão ser desativadas.

c. Salve o arquivo no caminho do diretório C:\TEMP\.
d. Copie o arquivo em OPERA6.INI.
e. Reinicie o espaço de trabalho do Rescue and Recovery para que as alterações sejam efetivadas.

Alterando o Comportamento dos Arquivos com Extensões Específicas

Você pode alterar o comportamento dos arquivos substituindo os valores no arquivo NORM1.INI. Para alterar o comportamento do arquivo pela extensão, faça o seguinte:

1. Feche o Opera e todas as janelas ativas do Opera, incluindo os arquivos de ajuda.
2. Abra o arquivo PREBOOT\OPERA\NORM1.INI para edição utilizando o processo RRUTIL, descrito em "Utilizando o RRUTIL.EXE" na página 20.
3. Localize a seção [File Types] do arquivo e, em seguida, procure a extensão com a qual deseja trabalhar. Por exemplo, você deseja que todos os arquivos .TXT sejam salvos na pasta IBMSHARE.
4. Localize a seguinte entrada: TEXT/PLAIN=2,,,,TXT,|

   Nota: Um valor de 2 instrui o navegador a exibir o texto no Opera. Um valor de 1 instrui o navegador a salvar o arquivo de destino na pasta IBMSHARE.
5. Continuando com o exemplo .TXT, altere a linha para que seja lida da seguinte forma:

   ```
   TEXT/PLAIN=1,,,,TXT,|
   ```
6. Salve o arquivo e coloque-o novamente utilizando o processo RRUTIL, conforme descrito em "Utilizando o RRUTIL.EXE" na página 20.
7. Reinicie o espaço de trabalho do Rescue and Recovery para que as alterações sejam efetivadas.

Incluindo um Endereço IP Estático

Para incluir um endereço IP Estático, você precisa alterar os arquivos a seguir.

1. Obtenha o arquivo \MININT\SYSTEM32 WINBOM.INI utilizando o processo RRUTIL, descrito em "Utilizando o RRUTIL.EXE" na página 20.
2. Inclua a seção [WinPE.Net] antes de [PnPDriverUpdate] no arquivo WINBOM.INI. Por exemplo, considere o seguinte arquivo: WINBOM.INI

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

```
[AppPreInstall]
```

Você deve incluir as seguintes linhas na seção [WinPE.Net].

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

Tabela 7. Entradas do Endereço IP Estático

Entrada	Descrição
Gateway	Especifica o endereço IP de um roteador IP. A configuração de um gateway padrão cria uma rota padrão na tabela de roteamento IP. **Sintaxe:** Gateway = *xxx.xxx.xxx.xxx*
IPConfig	Especifica o endereço IP que o Windows PE utiliza para conectar à rede. **Sintaxe:** IPConfig = *xxx.xxx.xxx.xxx*
StartNet	Especifica se deve iniciar os serviços de rede. **Sintaxe:** StartNet = *Yes* | *No*
SubnetMask	Especifica um valor de 32 bits que permite ao destinatário dos pacotes IP distinguir as partes de ID da rede e ID do host do endereço IP. **Sintaxe:** SubnetMask = *xxx.xxx.xxx.xxx*

3. Obtenha o arquivo PREBOOT\IBMWORK NETSTART.TBI utilizando o processo RRUTIL, descrito em "Utilizando o RRUTIL.EXE" na página 20.
4. Alterar

   ```
   factory -minint
   ```

   a

   ```
   factory -winpe
   ```
5. Comente as seguintes linhas:

   ```
   regsvr32 /s netcfgx.dll
   netcfg -v -winpe
   net start dhcp
   net start nla
   ```
6. Coloque os arquivos \IBMWORK NETSTART.TBI e \MININT\SYSTEM32 WINBOM.INI novamente utilizando o processo RRUTIL, descrito em "Utilizando o RRUTIL.EXE" na página 20.

Alterando a Resolução de Vídeo

Você pode alterar a resolução de vídeo alterando as configurações padrão da resolução do pré-desktop de 800 × 600 × 16 bits. Para alterar as configurações, faça o seguinte:

1. Obtenha o arquivo MININT\SYSTEM32\WINBOM.INI utilizando o processo RRUTIL, descrito em "Utilizando o RRUTIL.EXE" na página 20.
2. No arquivo WINBOM.INI, inclua as seguintes entradas:

   ```
   [ComputerSettings]
   DisplayResolution=800x600x16 or 1024x768x16
   In the file preboot\ibmwork\netstart.tbi change factory-minint to factory-winpe
   ```

Quando o ambiente do Rescue and Recovery for iniciado, você verá uma janela adicional durante a inicialização com o título ″Pré-instalação de Fábrica.″ Além disso, as cores serão reduzidas de milhares a 256.

3. Coloque novamente o arquivo MININT\SYSTEM32\WINBOM.INI utilizando o processo RRUTIL, descrito em “Utilizando o RRUTIL.EXE” na página 20.

Aplicativos de Inicialização

O ambiente do Rescue and Recovery Windows PE tem a capacidade de suportar um script de inicialização, programas ou programas customizados. Esses scripts ou programas serão processados antes de o ambiente do Rescue and Recovery Windows PE atingir a página principal da interface do PE.

O diretório para colocar o script ou programas é o Preboot\Startup. Os scripts ou programas deste diretório são processados alfanumericamente. Portanto, um script chamado A.BAT seria processado antes como 1.EXE.

Para colocar um script ou programa neste diretório, faça o seguinte:

1. Obtenha RRUTIL no site Lenovo Rescue and Recovery Administration Tools, no endereço:

   www.lenovo.com/ThinkVantage
2. Crie um diretório temporário.
3. No diretório \Temp, crie a seguinte árvore de diretórios, \preboot\startup.
4. Coloque o script ou programa no caminho \temp\preboot\startup.
5. Na linha de comandos, digite RRUTIL –p \Temp.
6. Para verificar se o script ou programa foi copiado com êxito, digite RRUTIL –g em uma linha de comandos. Isso gerará um arquivo chamado getlist.txt.
7. Examine o conteúdo do getlist.txt do diretório \preboot\startup. O script ou programa deverá ser listado nesta árvore.

Senhas

Há quatro opções de senha disponíveis na Área Pré-desktop. São elas:

- Senha principal ou pré-desktop
- ID e senha do usuário ou passphrase
- Senha de backup
- Sem senha

Senha Principal ou Pré-desktop

Você pode definir uma senha da Área Pré-desktop independente. Esta senha é definida pela interface da linha de comandos e será a única opção de senha disponível se o Client Security Solution não estiver instalado.

Você pode criar esta senha da Área de Pré-desktop utilizando o seguinte comando: C:\Program Files\IBM ThinkVantage\Client Security Solution\pe_setupmasterpwde.exe.

Os parâmetros para este comando são:

Tabela 8.

Parâmetro	**Descrição**
create password	Este parâmetro cria a senha real.

Tabela 8. (continuação)

Parâmetro	Descrição
verify password	Este parâmetro verifica se a senha é válida e se pode ser utilizada.
change currentPassword *newPassword*	Este parâmetro permite alterar a senha atual para outra.
exists	Este parâmetro verifica se a senha existe.
silent	Este parâmetro oculta todas as mensagens.
setmode values	0 = nenhuma autenticação requerida 1 = autenticação específica do usuário requerida 2 = senha principal requerida

Nota: Um Usuário limitado não pode alterar a senha; um administrador pode reconfigurar a senha para um usuário limitado.

ID e Senha do Usuário ou Passphrase

Esta opção utiliza o código do Client Security Solution para gerenciamento de senhas ou passphrases. O logon do Client Security solicitará ao usuário essa senha ou passphrase na inicialização da Área de Pré-desktop. Isso fornece melhor segurança para um ambiente multiusuário. Se um usuário efetuar logon utilizando o logon, esse usuário terá permissão para acessar apenas os arquivos desse usuário e nenhum arquivo de outro usuário.

Esta opção pode ser definida pela GUI do CSS ou por meio de scripts XML.

Senha de Backup

A senha de backup pode ser definida por meio da GUI Definir Senha ou da interface da linha de comandos rrcmd com backup especificado. A seguir, estão alguns exemplos:

```
rrcmd backup location=L name=mybackup password=pass
rrcmd basebackup location=L name=basebackup password=pass
rrcmd sysprepbackup location=L name="Sysprep Backup" password=pass
```

Sem Senha

Esta opção não utiliza autenticação e permite que o usuário entre na Área de Pré-desktop sem utilizar uma senha.

Acesso à Senha de ID

Há três opções para o acesso à senha:

- Senha principal
- ID e senha do usuário ou passphrase
- Sem senha

Senha Principal

A senha principal é uma senha única que permite acessar a Área Pré-desktop e os backups. Ela é definida utilizando a interface da linha de comandos e será a única opção de senha se o Client Security Solution não estiver instalado.

ID e Senha do Usuário ou Passphrase

Esta opção utiliza o código do Client Security Solution para gerenciamento de senhas ou passphrases. O GINA do Client Security Solution solicitará ao usuário essa senha ou passphrase na inicialização da Área de Pré-desktop. Isso fornece melhor segurança para um ambiente multiusuário. Se um usuário efetuar logon utilizando o GINA, esse usuário terá permissão para acessar apenas os arquivos desse usuário e de ninguém mais.

Nota: Isso inclui também as informações do arquivo de volume criptografado SecureDrive PrivateDisk do usuário.

Esta opção pode ser definida por meio da interface da linha de comandos ou na GUI.

Sem Senha

Esta opção não utiliza autenticação e permite que o usuário entre na Área de Pré-desktop sem utilizar uma senha.

Tipo de Restauração

A seguir, estão os métodos para restauração de arquivos:

- Resgate de arquivo
- Restauração de arquivo simples
- Sistema operacional e Appls
- Renovação
- Restauração completa
- Conteúdo de fábrica/Image Ultra Builder

Nota: O Rescue and Recovery não poderá capturar credenciais em cache para um usuário do domínio após uma restauração.

Resgate de Arquivo (Antes de Qualquer Restauração)

Esta função solicita ao usuário o local de armazenamento de backup e, em seguida, o usuário seleciona um backup. O ThinkVantage Rescue and Recovery deverá exibir então os arquivos que o usuário com logon efetuado tem autorização para acessar. O usuário seleciona então os arquivos e/ou pastas a serem resgatados. O sistema exibe então os locais disponíveis para os arquivos a serem resgatados, excluindo o HDD local. O usuário escolhe um destino com espaço suficiente e o sistema restaura os arquivos.

Restauração de Arquivo Simples

Esta função solicita ao usuário o local de Armazenamento de Backup e, em seguida, o usuário seleciona um backup. O ThinkVantage Rescue and Recovery deverá exibir então os arquivos que o usuário com logon efetuado tem autorização para acessar. O usuário seleciona então os arquivos e/ou pastas a serem restaurados e o sistema os restaurará para os seus locais originais.

Sistema Operacional e Apps

Esta função oferece ao usuário a opção de selecionar um backup e, em seguida o sistema exclui os arquivos definidos pela regras do osfilter.txt. Em seguida, restaura os arquivos definidos pelo OSFILTER.TXT a partir do backup selecionado.

Há também opções no arquivo tvt.txt que podem especificar que um programa seja executado antes ou após uma restauração; consulte as configurações e os valores de TVT.

Notas:

1. S.O. e Apps sempre utilizam Persistência de Senhas.
2. A restauração do S.O. e Apps não estão disponíveis no backup de CD/DVD.

Você pode incluir tarefas customizadas para serem executadas antes e após Backups e Restaurações. Consulte Apêndice B, "Configurações e Valores do TVT.TXT", na página 141 para obter as configurações de backup e de restauração.

Renovação

Ao selecionar para renovar o sistema, o programa Rescue and Recovery otimizará o desempenho do sistema fazendo um novo backup incremental e, em seguida, desfragmentando a unidade de disco rígido e os backups. Em seguida, restaura as configurações e os dados selecionados a partir de um backup de sua preferência. As operações de renovação ajudam a eliminar vírus, adwares e spywares enquanto mantêm as configurações e os dados atuais. Essas operações podem levar algum tempo.

Para renovar o sistema, conclua o seguinte procedimento:

1. Na interface do Rescue and Recovery, clique no ícone **Restore your system from a backup**. A tela Restore your system é exibida.
2. Na tela Restore your system, selecione **Rejuvenate your system**.
3. Escolha a unidade e o backup que deseja utilizar para renovar o sistema, concluindo o seguinte procedimento:
   a. Selecione a unidade apropriada no menu drop-down das unidades disponíveis. Os arquivos de backup na unidade selecionada são exibidos pela interface do Rescue and Recovery.
   b. Selecione o arquivo de backup que você deseja utilizar para renovar o sistema.
   c. Clique em **Next**.
   d. Confirme se o backup selecionado é aquele que você deseja utilizar para renovar o sistema e, em seguida, clique em **Next** para começar o processo de restauração. Você será lembrado para não desligar o computador durante esta operação.
   e. Clique em **OK** para continuar. Uma barra de progresso é exibida. Esta operação levará algum tempo.

Você pode incluir tarefas customizadas para serem executadas antes e após um Renovação. Consulte o Apêndice B, "Configurações e Valores do TVT.TXT", na página 141 para obter as configurações de renovação.

Nota: Os aplicativos instalados ou desinstalados depois que o backup selecionado foi criado podem ter de ser desinstalados novamente para que funcionem corretamente.
Atenção: Assegure-se de que o sistema esteja conectado a uma fonte de alimentação AC antes de iniciar um procedimento de backup, restauração, renovação ou arquivamento. Se essa instrução não for seguida, o resultado poderá ser perda de dados ou uma falha irrecuperável do sistema.

Restauração Completa

Esta função exclui todos os arquivos da unidade local e, em seguida, restaura os arquivos a partir do backup selecionado. Se a persistência de senhas estiver selecionada, então a senha mais recente disponível será restaurada.

Conteúdo de Fábrica/IUB (Image Ultra Builder)

Esta função apaga o disco rígido e reinstala todo o software pré-instalado na fábrica.

Persistência de Senhas

A tabela a seguir mostra considerações para decidir se deve utilizar Persistência de Senhas.

Tabela 9. Considerações sobre Persistência de Senhas

Problema	**Impacto se a Persistência de Senhas Estiver Ativada**
Se um usuário efetuar logon em um backup antigo com a conta e a senha atuais, então nenhum dos arquivos e das pastas do sistema do Arquivo Criptografado funcionará, pois esses arquivos foram criptografados em relação à conta e senha originais, e não à conta e senha persistentes.	• O usuário perderá dados do Sistema de Arquivos Criptografados. • Não é possível utilizar o Sistema de Arquivos Criptografados e a Persistência de Senhas ao mesmo tempo.
Se o usuário não existir nesse backup específico, então não terá nenhuma das pastas ou dos arquivos do usuário. Não existirão dados do aplicativo nem Favoritos do Internet Explorer.	• As configurações de documentos do ID do usuário serão perdidas. • Possível perda de dados.
A exclusão do usuário nas contas e senhas atuais removerá as informações de autenticação de todos os backups.	• O usuário não terá acesso aos dados.
Se um gerenciador ou um administrador de rede desejar excluir o acesso de vários ex-funcionários e desejar restaurar o backup básico para reconfigurar o sistema a fim de remover todas as contas de autenticação dos funcionários, os funcionários continuarão a ter acesso com a Persistência de Senhas.	• Não é recomendado pelas práticas e recomendações de manutenção de IDs de Usuários da Microsoft.

Ao restaurar a partir de uma unidade de disco rígido local, a senha atual será utilizada quando a Persistência de Senhas estiver selecionada. Ao restaurar a partir da USB ou da rede, a senha do backup mais recente será utilizada.

Reconfiguração da Senha de Hardware

O ambiente de reconfiguração da Senha de Hardware executa de forma independente do Windows e permitirá reconfigurar senhas esquecidas de inicialização e de unidade de disco rígido. Sua identidade é estabelecida pela resposta a um conjunto de perguntas que você cria ao se inscrever. Uma boa idéia é criar, instalar e inscrever este ambiente seguro o mais rápido possível antes que a senha seja esquecida. Não é possível reconfigurar senhas de hardware esquecidas até que tenham sido inscritas. Esta mídia de recuperação é suportada apenas nos computadores ThinkCentre e ThinkPad selecionados.

A criação deste ambiente não ajuda a recuperar senhas esquecidas do Windows ou uma senha associada ao espaço de trabalho do Rescue and Recovery. Com a criação deste ambiente, você está incluindo um dispositivo inicializável adicional no menu Dispositivo de Inicialização, a partir do qual é possível reconfigurar suas senhas de hardware esquecidas. Você acessa este menu pressionando F12 quando a senha de inicialização for solicitada.

Há três estágios envolvidos na configuração da implementação de senhas:

1. Construção do pacote
2. Implementação do pacote
3. Inscrição

Defina uma senha de Administrador ou Supervisor na BIOS, antes de começar este procedimento. Se você não tiver uma senha de Administrador ou de Supervisor da BIOS definida, o seu ambiente não estará tão seguro quanto possível. Todos os sistemas nos quais você planeja implementar o pacote de reconfiguração de senhas devem ter senha de Supervisor. Ao concluir este procedimento, sua senha de inicialização e de unidade de disco rígido serão as mesmas. Este procedimento é designado para ajudá-lo a concluir a tarefa de criar o ambiente seguro e ajudar a reconfigurar suas senhas esquecidas depois que o ambiente seguro for criado.

Construção do Pacote

Para criar um ambiente seguro, faça o seguinte:

1. No aplicativo de instalação de reconfiguração da senha de hardware, selecione o botão de rádio Criar Ambiente Seguro para Reconfigurar Senhas de Hardware.
2. Clique em OK. A janela Senha do Supervisor da BIOS é exibida.
3. No campo Digitar Senha do Supervisor, digite a senha do administrador ou do supervisor. Esta é a senha do Administrador ou do Supervisor que você definiu anteriormente na BIOS para proteger suas configurações de hardware.
4. Clique em OK. A janela Criar Chave é exibida.
5. Na área de geração de chave, execute um dos seguintes procedimentos:

   Na primeira vez em que você criar este ambiente segura, terá de criar uma nova chave. Uma chave é um recurso de segurança utilizado para autenticar sua identidade. Todas as tentativas subseqüentes de criar um ambiente seguro apresentarão a opção de utilizar a mesma chave criada na tentativa inicial se você optar por exportá-la ou criar uma chave diferente. Se estiver criando este ambiente para um computador apenas, será uma boa idéia gerar uma nova chave. Não é possível optar por gerar uma chave sempre que você criar um novo S.O. seguro. Entretanto, esta opção requer que você execute novamente o procedimento de inscrição em cada máquina. Se a mesma chave for utilizada, a inscrição não terá de ser novamente executada. Se você estiver criando este ambiente para vários computadores, talvez queira utilizar a mesma chave. Entretanto, é recomendável armazená-la em um local seguro, caso queira utilizar a mesma chave.

   Na área de geração da chave, execute um dos seguintes procedimentos:

   - Se esta for a primeira vez que estiver criando uma chave e planejar criar o ambiente seguro apenas neste computador, então selecione o botão de rádio Gerar Nova Chave.
   - Se esta for a primeira vez que estiver criando uma chave e desejar criar um ambiente seguro que possa ser implementado em outros computadores, então selecione o botão de rádio Gerar Nova Chave. Em seguida, selecione a

caixa de opções Exportar Chave para o Arquivo. Utilize o botão Navegar para definir onde deseja que a chave seja armazenada.

- Se você já criou uma chave e deseja utilizá-la para criar um ambiente seguro que possa ser implementado em outros computadores, então selecione o botão de rádio Importar Chave do Arquivo. Utilize o botão Navegar para definir onde a chave que você deseja utilizar está localizada. Você precisará da chave criada na opção acima.

Configure um sistema doador para cada tipo de sistema suportado ao implementar no Thinkpad, Thinkcentre e por idioma, por exemplo, francês, alemão, japonês. A finalidade é proteger o S.O. que é baseado na partição do Rescue and Recovery e deve ser diferente em cada sistema.

6. Na área de instalação, desmarque a caixa de opções Instalar automaticamente a reconfiguração da senha de hardware depois que ela for criada.
7. Clique em **OK**.
8. Clique em **OK** para que uma caixa de diálogo informe a você que o recurso Senha de Hardware não será ativado neste computador até que o pacote de instalação tenha sido executado.

   Para encontrar o caminho do arquivo executável, digite, no prompt da linha de comandos, cd %rr%\rrcd\passwordreset\pwdreset.exe.

Implementação do Pacote

Utilize a mídia de distribuição existente na empresa para implementar o pacote criado.

Inscrição

Para inscrever a reconfiguração da senha, faça o seguinte:

1. Execute o pwdreset.exe.
2. Clique em OK para reiniciar o computador. O computador será reiniciado e solicitará a digitação das senhas da BIOS. Digite as senhas da BIOS e, em seguida, clique em **Enter**. O computador reiniciará no ambiente seguro em que a janela de reconfiguração Bem-vindo à Senha de Hardware for exibida.
3. Selecione o botão de rádio **Instalar Reconfiguração de Hardware** se esta for a primeira vez que estiver criando o ambiente seguro ou se desejar reinscrever o computador e os discos rígidos.
4. Clique em **Avançar**. A janela de configuração de discos rígidos é exibida.
5. Na área de número de série do computador, selecione a caixa de opções Configuração além do computador que você deseja configurar.
6. Clique me **Avançar**. A janela Digitar Nova Senha de Inicialização é exibida.
7. No campo **Nova Senha de Inicialização**, digite a senha de inicialização que você deseja utilizar. Se já tiver uma senha de inicialização, ela será reconfigurada para a que você digitar nesse campo. Além disso, a senha da unidade de disco rígido será definida para a mesma senha.
8. Clique em **Avançar**. A janela Criar Perguntas e Respostas de Segurança é exibida.
9. Em cada um dos três campos de perguntas, digite a senha de inicialização que você deseja utilizar. Se você já tiver uma senha de inicialização, ela será reconfigurada para a que você digitar nesse campo. Além disso, a senha da unidade de disco rígido também será definida para a mesma senha.
10. Em cada um dos três campos de resposta, digite a resposta para cada pergunta. Você deverá saber cada resposta no caso de esquecer sua senha de inicialização e tentar reconfigurá-la.

11. Clique em **Avançar** e, em seguida, clique em **Concluir**. O computador reiniciará no ambiente Windows.

Aqui estão as mensagens de erro do instalador de reconfiguração da senha de hardware. As duas primeiras são títulos genéricos, utilizados em combinação com o restante das mensagens. Recomenda-se que você reinstale o produto em ambos os casos.

- **IDS_STRING_ERR** ″Erro″
- **IDS_STRING_ERR_INT** ″Erro Interno″
- **IDS_STRING_ERR_CMDLINE** ″A opção da linha de comandos que você digitou não foi reconhecida.\n\nUsage: scinstall [/postenroll | /biosreset | /newplanar]″
- **IDS_STRING_ERR_NOTSUPPORTED**

  A reconfiguração da senha de hardware não é suportada neste computador.
- **IDS_STRING_ERR_MEM**

  Este computador não tem memória suficiente para executar o recurso de reconfiguração da senha de hardware.
- **IDS_STRING_ERR_ENVAR**

  Uma variável de ambiente requerida está faltando. O Rescue and Recovery 3.0 (ou superior) deve ser instalado para utilizar o recurso de reconfiguração da senha de hardware.
- **IDS_STRING_ERR_MISSINGDLL**

  Um DLL requerido está faltando. O Rescue and Recovery 3.0 (ou superior) deve ser instalado para utilizar o recurso de reconfiguração da senha de hardware.
- **IDS_STRING_ERR_BIOSMAILBOX**

  Falha na atualização da BIOS para instalar o recurso de reconfiguração da senha de hardware. Desligue o computador e, em seguida, reinicie e tente novamente a instalação da reconfiguração da senha de hardware.
- **IDS_STRING_ERR_INSTALLRETRY**

  Esta operação não foi concluída com êxito. Para tentar novamente, desligue o computador, reinicie e execute novamente a instalação da reconfiguração da senha de hardware.
- **IDS_STRING_ERR_INSTALLPUNT**

  Esta operação não foi concluída com êxito. Para resolver o problema, consulte o administrador do sistema ou a documentação do Rescue and Recovery para obter detalhes.

Capítulo 4. Customização do Client Security Solution

Este capítulo utiliza termos definidos pelo TCG (Trusted Computing Group), referentes ao Módulo Confiável da Plataforma. Para obter uma explicação mais detalhada desses termos, consulte o site a seguir para obter referências e definições:

http://www.trustedcomputinggroup.org/

Vantagens do Chip de Segurança Embutido/Módulo Confiável da Plataforma

Um Módulo Confiável da Plataforma é um chip de segurança embutido projetado para fornecer funções relativas à segurança para o software que o utiliza. O chip de segurança embutido é instalado na placa-mãe de um sistema e se comunica por meio de um barramento de hardware. Os sistemas que incorporam um Módulo Confiável da Plataforma podem criar chaves criptográficas e critpografá-las para que possam ser decriptografadas apenas pelo mesmo Módulo Confiável da Plataforma. Este processo, normalmente chamado de *agrupamento* de chave, ajuda a proteger a chave contra divulgação. Em um sistema com um Módulo Confiável da Plataforma, o agrupamento de chave principal chamado SRK (Chave Raiz de Armazenamento), é armazenado dentro do próprio Módulo Confiável da Plataforma, para que a parte privada da chave nunca fique exposta. O chip de segurança embutido pode ainda armazenar outras chaves de armazenamento, chaves de assinatura, senhas e outras pequenas unidades de dados. Entretanto, há uma capacidade limitada de armazenamento no Módulo Confiável da Plataforma, portanto a SRK é utilizada para criptografar outras chaves de armazenamento fora do chip. Como a SRK nunca sai do chip de segurança embutido, ela forma a base do armazenamento protegido.

Quando os dados protegidos pelo Módulo Confiável da Plataforma são necessários, esses dados são transmitidos para o processamento pelo ambiente de hardware embutido seguro. Depois da autenticação e da decriptografia bem-sucedida, os dados não protegidos podem ser utilizados dentro do sistema.

Os sistemas que incorporam um Módulo Confiável da Plataforma são resistentes a ataques da mesma maneira que qualquer hardware é mais resistente a ataques do que software. Isso é especialmente importante ao alavancar as chaves criptográficas. As partes privadas de pares de chaves assimétricas são mantidas separadas da memória controladas pelo sistema operacional. O Módulo Confiável da Plataforma utiliza o seu próprio firmware interno e os circuitos lógicos para instruções de processamento, não contam com o sistema operacional e não se submetem às vulnerabilidades do software externo.

Nenhum sistema pode fornecer segurança perfeita, incluindo sistemas que utilizam a tecnologia do Módulo Confiável da Plataforma. O chip de segurança embutido é projetado para resistir à violação ou análise elétrica. Entretanto, a execução do tipo de análise necessária para descobrir segredos protegidos pelo Módulo Confiável da Plataforma requer acesso físico à máquina e ao hardware especializado adicional, tornando os segredos de uma plataforma ativada pelo chip de segurança embutido muito mais seguros do que aqueles em um sistema de software apenas. O aumento

da dificuldade em roubar segredos dos sistemas ajuda a aumentar o nível geral de segurança tanto individual como corporativo.

O chip de segurança embutido utiliza um processo opcional e requer um Administrador do Client Security Solution. O Módulo Confiável da Plataforma deverá estar inicializado, quer para um usuário individual ou um departamento corporativo de TI. As operações subseqüentes, como a capacidade de recuperar de uma falha da unidade de disco rígido ou de uma placa-mãe substituída, também são restritas ao Administrador do Client Security Solution.

Como o Client Security Solution Gerencia Chaves Criptográficas

As operações internas do Client Security Solution são descritas por duas atividades principais de implementação: Obter Direito à Propriedade e Inscrever Usuário. Durante a execução inicial do Assistente de Configuração do Client Security, os processos Obter Direito à Propriedade e Inscrever Usuário são executados durante a inicialização. O ID do usuário particular do Windows que concluiu o Assistente de Configuração do Client Security é o Administrador do Client Security Solution e é inscrito como um usuário ativo. Todo usuário que efetuar login no sistema será solicitado automaticamente a se inscrever no Client Security Solution.

- **Obter Direito à Propriedade - designar administrador do Client Security Solution**

  Um ID de usuário exclusivo do Administrador do Windows é designado como o único Administrador do Client Security Solution do sistema. As funções administrativas do Client Security Solution devem ser executadas por meio deste ID de usuário. A autorização do Módulo Confiável da Plataforma é a senha do Windows ou a passphrase do Client Security deste usuário.

  Nota: A única maneira de recuperar uma senha ou passphrase esquecida dos Administradores do Client Security Solution é desinstalar o software com permissões válidas do Windows ou limpar o chip de segurança na BIOS. De qualquer maneira, os dados protegidos pelas chaves associadas ao Módulo Confiável da Plataforma serão perdidos. O Client Security Solution fornece também um mecanismo opcional que permite a recuperação automática de uma senha ou passphrase esquecida, com base em uma challenge response de pergunta e resposta que faz parte da função Inscrever Usuário. O Administrador do Client Security Solution toma a decisão se deve utilizar o recurso ou não.

- **Inscrever Usuário**

  Depois que o processo Obter Direito à Propriedade for concluído e um Administrador do Client Security Solution for criado, uma Chave Básica do Usuário poderá ser criada para armazenar com segurança as credenciais do usuário do Windows atualmente conectado. Este design permite que vários usuários se inscrevam no Client Security Solution e alavanquem o único Módulo Confiável da Plataforma. As chaves de usuário são protegidas pelo chip de segurança, mas, na realidade, são armazenadas fora do chip, na unidade de disco rígido. Ao contrário de outras tecnologias de segurança, este design cria espaço na unidade de disco rígido como o fator de limite de armazenamento em vez da memória real criada no chip de segurança. Com este design, o número de usuários capazes de alavancar o mesmo hardware seguro é imensamente ampliado.

Obter Direito à Propriedade

A raiz da confiança do Client Security Solution é a SRK (Chave Raiz do Sistema). Esta chave assimétrica não migrável é gerada dentro do ambiente seguro do

Módulo Confiável da Plataforma e nunca é exposta ao sistema. A autorização para alavancar a chave deriva-se da conta do Administrador do Windows durante o comando “TPM_TakeOwnership”. Se o sistema estiver alavancando uma passphrase do Client Security, então a passphrase do Client Security do administrador do Client Security Solution será a autorização do Módulo Confiável da Plataforma; caso contrário, será a senha do Windows do Administrador do Client Security Solution.

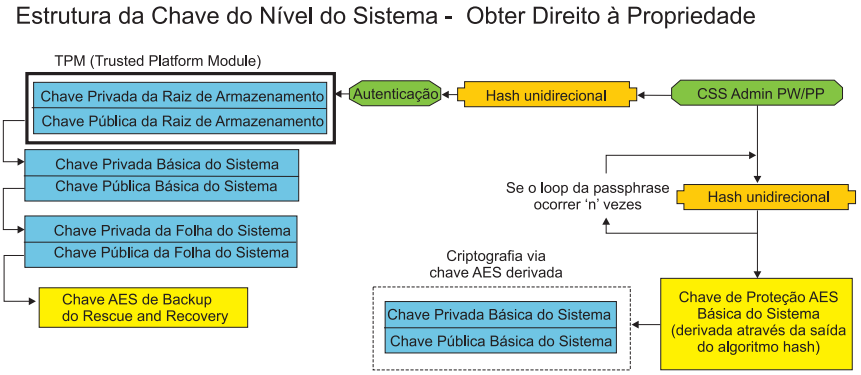

Figura 1.

Com a SRK criada para o sistema, outros pares de chaves podem ser criados e armazenados fora do Módulo Confiável da Plataforma, mas agrupados ou protegidos pelas chaves baseadas em hardware. Como o Módulo Confiável da Plataforma, que inclui a SRK é hardware e hardware pode ser danificado, um mecanismo de recuperação é necessário para garantir que um dano ao sistema não impeça a recuperação de dados.

Para recuperar um sistema, é criada uma Chave Básica do Sistema. Essa chave de armazenamento assimétrico migrável permitirá que o Administrador do Client Security Solution recupere a partir de uma troca da placa-mãe ou de uma migração planejada para outro sistema.

Para proteger a Chave Básica do Sistema, mas permitir que ela seja acessível durante a operação ou recuperação normal, duas instâncias da chave são criadas e protegidas por dois métodos diferentes. Primeiro, a Chave Básica do Sistema é criptografada com uma chave AES simétrica derivada do conhecimento da senha do Administrador do Client Security Solution ou da passphrase do Client Security. Esta cópia da Chave de Recuperação do Client Security Solution é exclusivamente para fins de recuperação de um Módulo Confiável da Plataforma limpo ou uma placa-mãe substituída devido a defeito de hardware.

A segunda instância da Chave de Recuperação do Client Security Solution é agrupada pela SRK para importá-la para a hierarquia de chaves. Essa instância dupla da Chave Básica do Sistema permite que o Módulo Confiável da Plataforma proteja os segredos vinculados a ele sob uso normal e permite uma recuperação de uma placa-mãe defeituosa por meio da Chave Básica do Sistema criptografada com uma chave AES desbloqueada pela senha do Administrador do Client Security Solution ou pela passphrase do Client Security.

A seguir, será criada uma Chave da Folha do Sistema. Esta chave de legado é criada para proteger os segredos ao nível do sistema, como a chave AES utilizada pelo Rescue and Recovery para proteger backups.

Inscrever Usuário

Para que os dados de cada usuário sejam protegidos pelo mesmo Módulo Confiável da Plataforma, cada usuário terá sua própria Chave Básica do Usuário criada. Essa chave de armazenamento assimétrica migrável também é criada duas vezes e protegida por uma chave AES simétrica, gerada a partir de cada senha do Windows do usuário ou passphrase do Client Security. A segunda instância da chave básica do usuário é então importada para o Módulo Confiável da Plataforma e protegida pela SRK do sistema. Consulte a Figura 2.

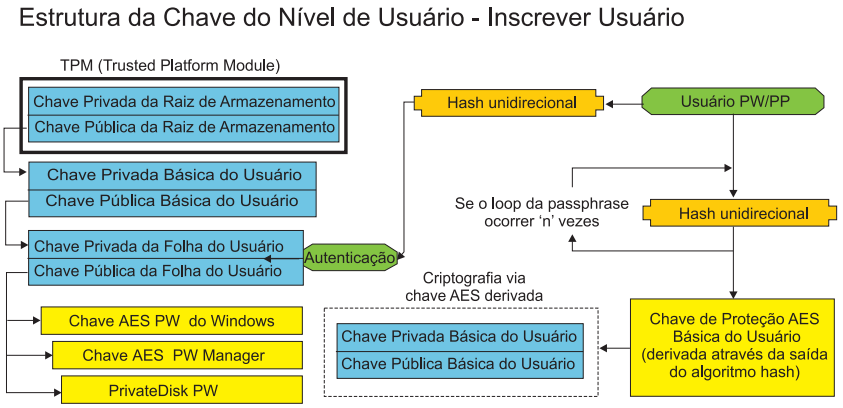

Figura 2.

Com a Chave Básica do Usuário criada, uma chave assimétrica secundária chamada de Chave da Folha do Usuário é criada para proteger segredos individuais, como a chave AES do Gerenciador de Senhas utilizada para proteger informações de logon da Internet, Senha do PrivateDisk utilizada para proteger dados e a Chave AES da Senha do Windows utilizada para proteger o acesso ao sistema operacional. O acesso à Chave da Folha do Usuário é controlado pela senha do Windows do usuário ou pela passphrase do Client Security Solution e é desbloqueada automaticamente durante o logon.

Emulação de Software

Se um sistema não tiver um Módulo Confiável da Plataforma, então será utilizada uma raiz de confiança baseada em software. A mesma funcionalidade estará disponível para o usuário, exceto que a segurança foi reduzida uma vez que a raiz da confiança será chaves baseadas em software. A SRK do Módulo Confiável da Plataforma é substituída por uma Chave RSA baseada em software e uma Chave AES para fornecer a proteção que o Módulo Confiável da Plataforma forneceu. A chave RSA agrupa a chave AES e a chave AES é utilizada para criptografar a próxima chave RSA da hierarquia.

Troca da Placa-mãe

Uma troca da placa-mãe pressupõe que a SRK antiga às quais as chaves estavam ligadas não são mais válidas e outra SRK é necessária. Isso pode acontecer também se o Módulo Confiável da Plataforma for limpo por meio da BIOS.

O Administrador do Client Security Solution é requerido para ligar as credenciais do sistema a uma nova SRK. A Chave Básica do Sistema precisará ser

decriptografada por meio da Chave de Proteção AES Básica do Sistema, derivada das credenciais de autorização do Administrador do Client Security Solution. Consulte a Figura 3.

Nota: Se um Administrador do Client Security Solution for um domínio, o ID do usuário e a senha desse ID de usuário foram alterados em uma máquina diferente; a senha utilizada pela última vez ao efetuar logon no sistema que precisa de recuperação deverá ser conhecida para decriptografar a Chave Básica do Sistema para recuperação. Por exemplo, durante a implementação de um Administrador do Client Security Solution, um ID de usuário e uma senha serão configurados; se a senha deste usuário for alterada em uma máquina diferente, então a senha original definida durante a implementação será a autorização necessária para a recuperação do sistema.

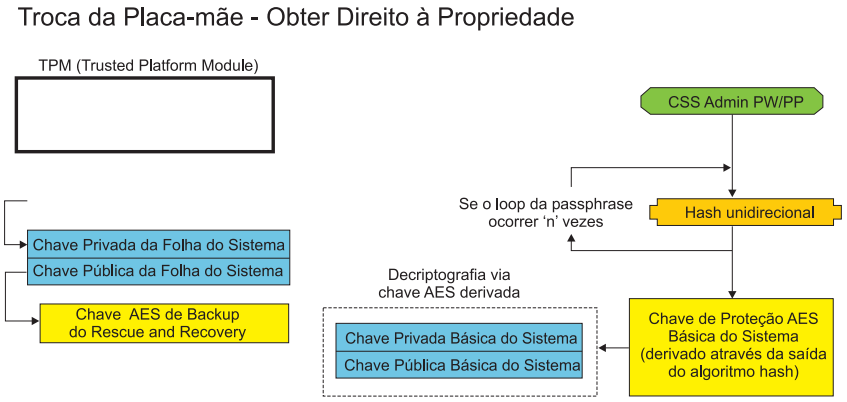

Figura 3.

Siga estas etapas para executar a troca da placa-mãe:

1. O Administrador do Client Security Solution efetua logon no sistema operacional.
2. O código executado pelo logon (cssplanarswap.exe) reconhece que o chip de segurança está desativado e requer a reinicialização para ser ativado. (Esta etapa pode ser evitada ativando o chip de segurança por meio da BIOS).
3. O sistema é reinicializado e o chip de segurança é ativado.
4. O Administrador do Client Security Solution efetua logon; o novo processo Obter Direito à Propriedade é concluído.
5. A Chave Básica do Sistema é decriptgrafada utilizando a Chave de Proteção AES Básica do Sistema derivada pela autenticação do Administrador do Client Security Solution. A Chave Básica do Sistema é importada para a nova SRK e restabelece a Chave de Página do Sistema e todas as credenciais protegidas por ela.
6. Agora, o sistema está recuperado.

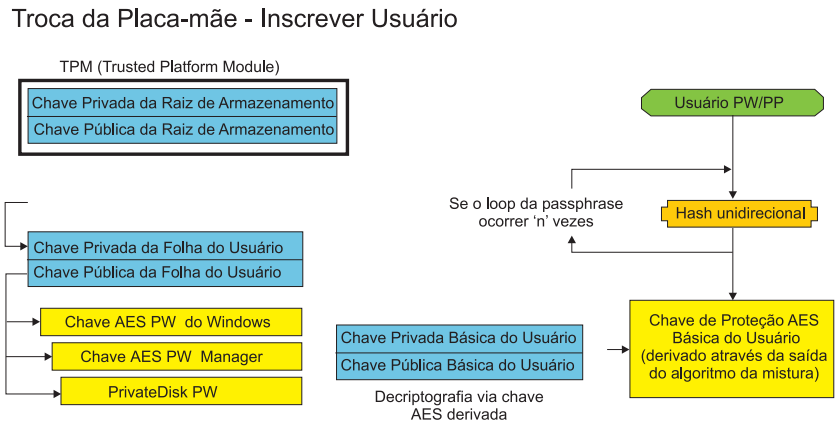

Figura 4.

À medida que cada usuário efetua logon no sistema, a Chave Básica do Usuário é decriptografada automaticamente por meio da Chave de Proteção AES Básica do Usuário, derivada da autenticação do Usuário e importada para a nova SRK criada por meio do Administrador do Client Security Solution.

Esquema do XML

A finalidade do script XML é permitir que os Administradores de TI criem scripts customizados que possam ser utilizados para implementar o Client Security Solution. Todas as funções disponíveis no Assistente de Configuração do Client Security Solution também estão disponíveis no script. Os scripts podem ser protegidos pelo executável xml_crypt_tool (com uma senha (criptografia de AES) ou uma ambigüidade). Depois de criados, a máquina virtual (vmserver.exe) aceita os scripts como entrada. A máquina virtual chama as mesmas funções do Assistente de Configuração para configurar o software.

Uso

Todos os scripts consistem em uma tag para especificar o tipo de codificação XML, o esquema XML e, pelo menos, uma função a ser executada. O esquema é utilizado para validar o arquivo XML e verificar se os parâmetros necessários estão presentes. O uso do esquema não é obrigatório atualmente. Cada função é colocada em uma tag de função. Cada função contém uma ordem e isso especifica em qual ordem o comando será executado pela máquina virtual (vmserver.exe). Da mesma forma, cada função tem um número de versão. Atualmente todas as funções estão na versão 1.0. Para clareza, cada um dos scripts do exemplo a seguir contém apenas uma função. Entretanto, na prática, um script muito provavelmente conteria várias funções. O Assistente de Configuração do Client Security Solutions pode ser utilizado para criar um script. Consulte “Assistente do Client Security” na página 159 (consulte a documentação do assistente de configuração para obter detalhes).

Nota: Se o parâmetro <DOMAIN_NAME_PARAMETER> for omitido em alguma das funções que requerem um nome de domínio, então será utilizado o o nome do computador padrão do sistema.

Exemplos

AUTO_ENROLL_ADMIN_FOR_RNR_ONLY

Este comando permite que o Administrador do sistema gere as chaves de segurança necessárias para criptografar backups com o Rescue and Recovery. Este comando deve ser executado apenas uma vez por sistema; ele não deve ser executado para cada usuário, apenas para o Administrador.

Nota: Apenas para instalações do Rescue and Recovery, um Administrador deverá ser designado como o Proprietário do TPM se os backups tiverem de ser criptografados com o TPM. Utilize o seguinte arquivo de script para designar automaticamente um ID de usuário e uma senha do Administrador. Esse ID de usuário e senha do Windows serão utilizados para fins de recuperação do TPM. (Todas as outras funções de script XML do CSS não serão aplicáveis se apenas o Rescue and Recovery estiver instalado).

- **USER_NAME_PARAMETER**

  O ID de usuário do Windows do usuário Administrador.
- **DOMAIN_NAME_PARAMETER**

  O nome de domínio do usuário Administrador.
- **RNR_ONLY_PASSWORD**

  A senha do Windows do usuário 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>WinAdminName</USER_NAME_PARAMETER
          <DOMAIN_NAME_PARAMETER>MyCorp</DOMAIN_NAME_PARAMETER>
          <RNR_ONLY_PASSWORD>WinPassw0rd<RNR_ONLY_PASSWORD>
         </FUNCTION>
</CSSFile>
```

ENABLE_TPM_FUNCTION

Este comando ativa o Módulo Confiável da Plataforma e utiliza o argumento SYSTEM_PAP. Se o sistema já possui uma senha de Administrador/Supervisor da BIOS definida, então este argumento deverá ser fornecido. Caso contrário, este comando é 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 comando utiliza o argumento SYSTEM_PAP. Se o sistema já possui uma senha de Administrador/Supervisor da BIOS definida, então este argumento deverá ser fornecido. Caso contrário, este comando é 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>password</SYSTEM_PAP>
         </FUNCTION>
</CSSFile>
```

ENABLE_ENCRYPT_BACKUPS_FUNCTION

Quando você utiliza o Rescue and Recovery, este comando ativa a proteção dos backups com o 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

Ao utilizar o Rescue and Recovery para proteger os backups, este comando desativa a proteção dos backups com o 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 comando ativa o gerenciador de senhas para todos os usuários do 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 comando ativa o Logon do 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

Se o ThinkVantage Fingerprint Software estiver instalado, este comando ativará o Logon.

```
<?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

Se o ThinkVantage Fingerprint Software estiver instalado, este comando ativará o Logon com suporte à Troca Rápida de Usuário.

```
<?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

Se o Logon do ThinkVantage Fingerprint Software ou do Client Security Solution estiver ativado, este comando desativará os Logons do ThinkVantage Fingerprint Software e do 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 comando grava um sinalizador que o Client Security Solution lê para determinar se deve utilizar a passphrase do Client Security ou uma senha do 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 comando ativa o SafeGuard PrivateDisk a ser utilizado no sistema. Cada usuário deve ainda ser especificamente configurado para utilizar o Safeguard PrivateDisk pelo 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 comando grava um sinalizador que o Client Security Solution lê para determinar quem é o usuário Administrador do Client Security Solution. Os parâmetros são:

- **USER_NAME_PARAMETER**

  O nome de usuário do usuário Admin.
- **DOMAIN_NAME_PARAMETER**

  O nome de domínio do usuário Admin.

```
<?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 comando permite que um determinado usuário utilize o PrivateDisk. Os parâmetros são:

- **USER_NAME_PARAMETER**

  O nome de usuário do usuário para ativar o PrivateDisk.
- **DOMAIN_NAME_PARAMETER**

  O nome de domínio do usuário para ativar o PrivateDisk.
- **PD_VOLUME_SIZE_PARAMETER**

  O tamanho do volume do PrivateDisk em megabytes.
- **PD_VOLUME_PATH_PARAMETER**

  O caminho do volume do PrivateDisk a ser criado.
- **PD_VOLUME_NAME_PARAMETER**

  O nome do volume do PrivateDisk a ser criado. Se o valor PD_USE_DEFAULT_OPTION for especificado, então um valor padrão será automaticamente utilizado.
- **PD_VOLUME_DRIVE_LETTER_PARAMETER**

  A letra da unidade do volume do PrivateDisk a ser criado. Se o valor PD_USE_DEFAULT_OPTION for especificado, então um valor padrão será automaticamente utilizado.
- **PD_VOLUME_CERT_PARAMETER**

  Se o valor PD_USE_CSS_CERT for transmitido, então o PrivateDisk criará um novo certificado ou utilizará um certificado existente e o protegerá com o CSP do Client Security Solution. A montagem/desmontagem deste volume estará ligada ao CSP em vez da senha do Windows/passphrase do CSS. Se o valor PD_USE_DEFAULT_OPTION for especificado, então nenhum certificado será utilizado e o padrão será a senha do Windows/passphrase do CSS do usuário.
- **PD_USER_PASSWORD**

  A senha que o Client Security Solution transmite ao PrivateDisk para montar/criar o volume do PrivateDisk. Se o valor PD_RANDOM_VOLUME_PWD for especificado, então o Client Security Solution gerará uma senha de volume aleatória.
- **PD_VOLUME_USER_PASSWORD_PARAMETER**

  Uma senha específica do usuário para montar o volume do PrivateDisk. Essa senha destina-se a um backup da senha do PD_USER_PASSWORD. Se, por qualquer motivo, o Client Security Solution falhar no futuro, o valor transmitido

para este argumento será independente do Client Security Solution. Se o valor PD_USE_DEFAULT_OPTION for especificado, então nenhum valor será utilizado.

```
<?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 comando inicializa o sistema no Client Security Solution a ser utilizado no sistema. Todas as chaves em todo o sistema são geradas por meio desta chamada de função. Os parâmetros são:

- **NEW_OWNER_AUTH_DATA_PARAMETER**

  A senha do proprietário inicializa o sistema. Se a senha do proprietário não for definida, o valor transmitido para este argumento se tornará a nova senha do proprietário. Se uma passphrase do proprietário já estiver definida e o administrador utilizar a mesma senha, então ela poderá ser transmitida. Nesse caso, em que o admin deseja utilizar uma nova passphrase do proprietário, então a senha desejada deverá ser transmitida neste parâmetro.

- **CURRENT_OWNER_AUTH_DATA_PARAMETER**

  A senha atual do proprietário do sistema. Se o sistema já tiver uma senha do proprietário 5.4x, então este parâmetro deverá ser transmitido na senha 5.4x. Caso contrário, se uma nova senha do proprietário for desejada, a senha atual do proprietário deverá ser transmitida neste parâmetro. Se nenhuma alteração for desejada, então o valor NO_CURRENT_OWNER_AUTH deverá ser transmitido.

```
<?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>pass1word</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 comando altera a autorização do administrador do Client Security Solution e atualiza as chaves do sistema de acordo. Todas as chaves em todo o sistema são regeneradas por meio desta chamada de função. Os parâmetros são:

- NEW_OWNER_AUTH_DATA_PARAMETER

  A nova senha do proprietário do Módulo Confiável da Plataforma.
- CURRENT_OWNER_AUTH_DATA_PARAMETER

  A senha atual do proprietário do Módulo Confiável da Plataforma.

```
<?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>newPassWord</NEW_OWNER_AUTH_DATA_
              PARAMETER>
          <CURRENT_OWNER_AUTH_DATA_PARAMETER>oldPassWord</CURRENT_OWNER_AUTH
               _DATA_PARAMETER>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENROLL_USER_FUNCTION

Este comando inscreve um determinado usuário para utilizar o Client Security Solution. Esta função cria todas as chaves de segurança específicas de um determinado usuário. Os parâmetros são:

- **USER_NAME_PARAMETER**

  O nome de usuário do usuário a ser inscrito.
- **DOMAIN_NAME_PARAMETER**

  O nome de domínio do usuário a ser inscrito.
- **USER_AUTH_DATA_PARAMETER**

  A senha do Windows/passphrase do Módulo Confiável da Plataforma com as quais criar as chaves de segurança do usuário.
- **WIN_PW_PARAMETER**

  A senha do 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>myCssUserPassPhrase</USER_AUTH_DATA_PARAMETER>

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

USER_PW_RECOVERY_FUNCTION

Este comando configura uma determinada recuperação de senha do usuário do Módulo Confiável da Plataforma. Os parâmetros são:

- **USER_NAME_PARAMETER**

  O nome de usuário do usuário a ser inscrito.
- **DOMAIN_NAME_PARAMETER**

  O nome de domínio do usuário a ser inscrito.
- **USER_PW_REC_QUESTION_COUNT**

  O número de perguntas às quais o usuário deve responder.
- **USER_PW_REC_ANSWER_DATA_PARAMETER**

A resposta armazenada para uma determinada pergunta. Observe que o nome real deste parâmetro está concatenado ao número correspondente da pergunta a que ele responde. Consulte o exemplo deste comando abaixo.

- **USER_PW_REC_STORED_PASSWORD_PARAMETER**

  A senha armazenada apresentada ao usuário depois que todas as perguntas forem respondidas corretamente.

```
<?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>Test1</USER_PW_REC_ANSWER_DATA_PARA
              METER>
          <USER_PW_REC_ANSWER_DATA_PARAMETER>Test2</USER_PW_REC_ANSWER_DATA_PARA
              METER>
          <USER_PW_REC_ANSWER_DATA_PARAMETER>Test3</USER_PW_REC_ANSWER_DATA_PARA
              METER>
          <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>Pass1word</USER_PW_REC_STORED_PASS
              WORD_PARAMETER>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

SET_WIN_PE_LOGON_MODE_FUNCTION

Este comando grava um sinalizador que o programa lê para determinar se deve exigir uma autorização do usuário ao entrar no ambiente do Windows PE. O parâmetro é:

- **WIN_PE_LOGON_MODE_AUTH_PARAMETER**

  As duas opções válidas são:

  – 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. Customização do System Migration Assistant

Há duas partes customizáveis do System Migration Assistant:

- Editando ou modificando um arquivo de comando
- Migrando configurações adicionais do aplicativo

Criando um Arquivo de Comando

Durante a fase de captura, o SMA lê o conteúdo do arquivo de comando e arquiva as configurações. Esta seção contém informações sobre arquivos de comando e as instruções que elas podem conter.

O System Migration Assistant fornece um arquivo de comando padrão (command.xml) que você pode utilizar como um gabarito para criar um arquivo de comando customizado. Se você instalou o SMA no local padrão, este arquivo estará localizado no diretório D:\%RR%\migration\bin.

Nota: O System Migration Assistant 5.0 utiliza tecnologia XML para descrever os comandos do arquivo de comando.

Considere os seguintes pontos referente aos arquivos de comando do SMA 5.0:

- O arquivo de comando segue o XML versão 1.0 sintaxe v. O arquivo de comando faz distinção entre maiúsculas e minúsculas.
- Cada seção de comandos e parâmetros deve começar com <TagName> e terminar com </TagName> e seu valor deve ser descrito entre essas tags.
- Os erros de sintaxe podem causar um erro ao executar o SMA. Se o SMA encontrar um erro, ele gravará o erro no arquivo de log e continuará a operação. Dependendo da gravidade do erro, os resultados finais poderão ser falhos.

Comandos do Arquivo de Comando

A tabela a seguir contém informações sobre os comandos, com exceção daqueles referentes à migração de arquivos ou ao registro, que pode ser utilizado em um arquivo de comando:

Tabela 10.

Comando	Parâmetros	Valores de Parâmetro e Exemplos

<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 selecionar uma configuração de desktop, defina o parâmetro como "true". Caso contrário, defina o parâmetro como "false" ou deixe-o sem especificação.
		
		Por exemplo:
		`<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 selecionar uma configuração de desktop, defina o parâmetro como "true". Caso contrário, defina o parâmetro como "false" ou deixe-o sem especificação.
		
		Por exemplo:
		`<Network>`
		`<computer_name>true<computer_name>`
		`<mapped_drives>false</mapped_drives>`
		`</Network>`

<Applications>	<Application>
	
	Consulte o *ThinkVantageSystem Migration Assistant User's Guide* para obter uma lista de todos os aplicativos suportados.
		Por exemplo:
		`<Applications>`
		`<Application>Lotus Notes</Application>`
		`<Application>Microsoft Office</Application>`
		`<//Applications>`
		
		ou
		`<Applications>`
		`<Application>$(all)</Applications>`

<Registries>	• <Registry> • <hive> • <keyname> • <value>	Para capturar ou aplicar as configurações de registro, especifique a seção, o nome da chave e o valor como os parâmetros do arquivo de comando.

Tabela 10. (continuação)

Comando	Parâmetros	Valores de Parâmetro e Exemplos

<IncUsers>	<UserName>	Para capturar todos os perfis de usuário, defina $(all) ou utilize * como um caractere curinga para todos os usuários. Caso contrário, especifique usuários individualmente.
		
		Os seguintes caracteres curinga estão disponíveis.
		• * para um caractere curinga de comprimento variável
		• % para um caractere curinga de comprimento fixo (1 caractere)
		
		Por exemplo:
		`<IncUsers>`
		`<UserName>administrator</UserName>`
		`<UserName>domain\Jim</UserName>`
		`</IncUsers>`

<ExcUsers>	<UserName>	Para excluir usuário do processo de migração, especifique o nome de domínio e o nome de usuário do usuário. Os seguintes caracteres curinga estão disponíveis. • * para um caractere curinga de comprimento variável • % para um caractere curinga de comprimento fixo (1 caractere)

<Printers>	<Printer>
	
	<PrinterName>
		Esta instrução de controle é efetiva para o computador de origem e de destino.
		
		Para capturar todas as impressoras, defina o parâmetro como *&(all)*. Caso contrário, especifique cada impressora individualmente. Para capturar apenas a impressora padrão, defina o parâmetro como *&(DefaultPrinter)*.
		
		Por exemplo:
		`<Printers>`
		`  <Printer>&(all)</Printer>`
		`</Printers>`
		
		`<Printers>`
		`  <Printer>`
		`  <PrinterName>IBM 5589-L36</PrinterName>`
		`  </Printer>`
		`</Printers>`
		
		`<Printers>`
		`  <Printer>&(DefaultPrinter)</Printer>`
		`</Printers>`

Tabela 10. (continuação)

Comando	Parâmetros	Valores de Parâmetro e Exemplos
<MISC>	<bypass_registry>	Para cancelar a seleção de todas as configurações de registro, defina como “true”. Caso contrário, defina como “false” ou deixe-o sem especificação.
	<overwrite existing files>	Para sobrescrever arquivos existentes, defina como “true”. Caso contrário, defina como “false” ou deixe-o sem especificação.
	<log_file_location>	Para especificar o diretório no qual o SMA grava arquivos de log, digite um nome completo de diretório. Você pode especificar um diretório compartilhado em outro sistema. Se você não definir este parâmetro, o SMA gravará arquivos de log em d:/InstDir/, em que d é a letra da unidade de disco rígido e /InstDir/ é o diretório onde o SMA está instalado.
	<temp_file_location>	Para especificar o diretório no qual o SMA grava arquivos temporários, digite um nome completo de diretório. Você pode especificar um diretório compartilhado em outro sistema. Se você não definir este parâmetro, o SMA gravará arquivos temporários em d:/InstDir/etc/data, em que d é a letra da unidade de disco rígido e /InstDir/ é o diretório onde o SMA está instalado.
	<resolve_icon_links>	Para copiar apenas os ícones que possuem links ativos, defina como “true”. Caso contrário, defina o parâmetro como “false” ou deixe-o sem especificação.

Comandos de Migração de Arquivos

O SMA processa comandos de migração de arquivos na seguinte ordem: comandos de inclusão de arquivos são executados primeiro; em seguida, são executados comandos de exclusão de arquivos para os arquivos de inclusão.

O SMA selecionará e cancelará a seleção de arquivos com base no local original dos arquivos e pastas no computador de origem. As instruções de redirecionamento são armazenadas no perfil e são interpretadas durante a fase de aplicação.

O processamento de nomes de arquivos e diretórios não faz distinção entre maiúsculas e minúsculas.

A tabela a seguir contém informações sobre comandos de migração de arquivos. Todos os comandos de migração de arquivos são opcionais.

Tabela 11.

Comando	Parâmetro	O que ele faz

<FilesAndFolders>	<run>	Para capturar ou aplicar migração de arquivos, defina o parâmetro como “true”. Caso contrário, defina o parâmetro como “false” ou deixe-o sem especificação.
		
		Por exemplo:
		`<FilesAndFolders>`
		`<run>true</run>`
		`</FilesAndFolders>`

<Exclude_drives>	<Drive>	Especifique a letra da unidade para excluir unidades de serem varridas.
		
		Por exemplo:
		`<ExcludeDrives>`
		`<Drive>D</Drive>`
		`<Drive>E</Drive>`
		`</ExcludeDrive>`

Tabela 11. (continuação)

Comando	Parâmetro	O que ele faz

Inclusions	<IncDescriptions>
	<Description>
	<DateCompare>
	<Operand>
	<Date>
	<SizeCompare>
	<Operand>
	<Size>
	<Dest>
	<Operation> em que
	• <Description> é o nome completo do arquivo. Você pode utilizar caractere curinga para o nome do arquivo e o nome da pasta.
	• <DateCompare> é um parâmetro opcional que especifica arquivos baseados na data em que foram criados.
	– <Operand> é NEWER ou OLDER.
	– <Date> é a data da linha de base no formato mm/dd/aaaa.
	• <SizeCompare> é o parâmetro opcional para selecionar arquivos baseados no tamanho.
	– <Operand> é LARGER ou SMALLER.
	– <Size> é o tamanho do arquivo em MB.
	• <Dest> é um parâmetro opcional que especifica o nome da pasta de destino no sistema de destino em que os arquivos serão gravados.
	• <Operation> é um parâmetro opcional que especifica como o caminho do arquivo deve ser manipulado. Especifique um dos seguintes:
	– P mantém o caminho do arquivo e recria o arquivo no sistema de destino, começando no local especificado pelo parâmetro <Dest>.
	– R remove o caminho do arquivo e coloca o arquivo diretamente no local especificado pelo parâmetro <Dest>.
		Procura por todos os arquivos correspondentes nos diretórios especificados.
		Por exemplo:
		Exemplo 1
		`<IncDescription>`
		`<Description>c:\MyWorkFolder\ls</Description>`
		`</IncDescription>`
		Nota: Nota: Para especificar o nome da pasta, inclua .\. no final da descrição
		Exemplo 2
		`<IncDescription>`
		`<Description>C:\MyWorkFolder\*.*</Description>`
		`<DateCompare>`
		`<Operand>NEWER</Operand>`
		`<Date>07/31/2005</Date>`
		`</DateCompare>`
		`</IncDescription>`
		Exemplo 3
		`<IncDescription>`
		`<Description>C:\MyWorkFolder/*.*</Description>`
		`<SizeCompare>`
		`<Operand>SMALLER</Operand>`
		`<Size>200</Size>`
		`</SizeCompare>`
		`</IncDescription>`
		Exemplo 4
		`<IncDescription>`
		`<Description>C:\MyWorkFolder\*.*</Description>`
		`<Dest>D:\MyNewWorkFolder</Dest>`
		`<Operation>`
		`<IncDescription>`

Tabela 11. (continuação)

Comando	Parâmetro	O que ele faz

<Exclusions>	<ExDescriptions>
	<Description>
	<DateCompare>
	<Operand>
	<Date>
	<SizeCompare>
	<Operand>
	<Size> em que
	• <Description> é o nome completo do arquivo ou o nome da pasta. Pode conter caractere curinga para o nome do arquivo e o nome da pasta.
	• DateCompare> é um comando opcional que você pode utilizar para selecionar arquivos baseados na data em que foram criados.
	– <Operand> é NEWER ou OLDER.
	– <Date> é a data da linha de base no formato mm/dd/aaaa.
	• <SizeCompare> Parâmetro opcional para selecionar arquivos baseados no tamanho.
	– <Operand> é LARGER ou SMALLER.
	– <Size> é o tamanho do arquivo em MB.
		Cancela a seleção de todos os arquivos correspondentes em um diretório especificado.
		Por exemplo:
		Exemplo 1
		`<ExDescription>`
		`<Description>C:\YourWorkFolder</Description>`
		`</ExDescription>`
		Exemplo 2
		`<ExDescription>`
		`<Description>C:\YourWorkFolder</Description>`
		`<DateCompare>`
		`<Operand>OLDER</Operand>`
		`<Date>07/31/2005</Date>`
		`</DateCompare>`
		`</ExDescription>`
		Exemplo 3
		`<ExDescription>`
		`<Description>C:\YourWorkFolder</Description>`
		`<SizeCompare>`
		`<Operand>LARGER</Operand>`
		`<Size>200</Size></SizeCompare>`
		`</ExDescription>`

Exemplos de Comandos de Migração de Arquivos

Esta seção contém exemplos de comandos de migração de arquivos. Esses exemplos demonstram como combinar comandos de inclusão e exclusão de arquivos para refinar a seleção de arquivos. Apenas as seções de manipulação de arquivos do arquivo de comandos são mostradas.

Selecionando Arquivos Durante a Fase de Captura

Esta seção contém três exemplos de código utilizados para selecionar arquivos durante a fase de captura.

Exemplo 1

O exemplo de código a seguir seleciona todos os arquivos com uma extensão .doc (documentos do Microsoft Word) e os relocaliza no diretório “d:\My Documents”. Em seguida, exclui todos os arquivos que estão no diretório d:\No_Longer_Used

```
<IncDescription>
<Description>*:\*.doc/s</Description>
<Dest>d:\My Documents</Dest>
```

```
<Operation>r</Operation>
<IncDescription>
</Inclusions>
<Exclusions>
<ExcDescription>
<Description>d:\No_Longer_Used\</Description>
</ExcDescription>
</Exclusions>
```

Exemplo 2

O exemplo de código a seguir seleciona o conteúdo da unidade, excluindo todos os arquivos localizados na raiz da unidade d e todos os arquivos com uma extensão .tmp.

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

Exemplo 3

O exemplo de código a seguir seleciona o conteúdo inteiro da unidade c, excluindo todos os arquivos localizados em %windir% que especifica o diretório do Windows.

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

Exemplo 4

O exemplo de código a seguir seleciona o conteúdo inteiro da pasta %USERPROFILE% que é o Caminho de Perfil do Usuário do usuário de logon atual, excluindo todos os arquivos com uma extensão .dat e uma subpasta "Configurações Locais".

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

Migrando Configurações Adicionais do Aplicativo

Nota: Para criar arquivos de aplicativos customizados, você deve ter um conhecimento perfeito do aplicativo, incluindo os locais de armazenamento de configurações customizadas. Por padrão, o SMA está pré-configurado para migrar configurações para vários aplicativos. Para obter uma lista de aplicativos

suportados pelo SMA, consulte o *System Migration Assistant User's Guide*. Talvez você queira criar um arquivo de aplicativo customizado para migrar as configurações para aplicativos adicionais.

Este arquivo deve ser chamado application.xml ou application.smaapp e deve estar localizado no d:\%RR%\Migration\bin\Apps, em que *Apps* especifica o aplicativo e d é a letra da unidade de disco rígido. Será dada prioridade ao application.smaapp quando existirem os arquivos de aplicativos customizados application.smaapp e application.xml do mesmo aplicativo.

Para suportar um novo aplicativo, você pode copiar um arquivo de aplicativo existente e fazer as alterações necessárias. Por exemplo, Microsoft_Access.xml é um arquivo de aplicativo existente.

Considere os seguintes pontos sobre os arquivos de aplicativos:

- *application*.xml
  - Por padrão, quando o System Migration Assistant estiver instalado, existirá apenas o application.xml.
  - A <tag> delimitada por "<!-" e "->" é tratada como comentário. Por exemplo:

    ```
    <!--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 comando deve ser descrito em uma seção separada.
  - Cada seção começa com um comando delimitado por tags, por exemplo, <AppInfo> ou <Install_Directories>. Você pode digitar um ou mais campos em uma seção; cada campo deve estar em uma linha separada.
  - Se o arquivo de aplicativo contiver erros de sintaxe, o SMA continuará a operação e gravará os erros no arquivo de log

A Tabela 12 mostra informações sobre arquivos de aplicativos:

Tabela 12.

Seção	Comando	Valor	O que ele faz
<Applications>			
	<Family>	Uma cadeia de texto. Os espaços à esquerda são ignorados; não coloque a cadeia de texto entre aspas.	Especifica o nome não específico da versão do aplicativo. Ao executar o SMA no modo de batch, você utiliza esta cadeia na seção de aplicativos do arquivo de comando. Por exemplo: `<Family>adobe Acrobat Reader</Family>`
	<SMA_Version>	Um valor numérico.	Especifica o número da versão do SMA. Por exemplo, `<SMA_Version>SMA 5.0</SMA_Version`
	<App>	*ShortName* em que ShortName é um nome abreviado específico da versão de um aplicativo.	Especifica um nome abreviado específico da versão de um ou mais aplicativos. Por exemplo, `<APP>Acrobat_Reader_50</APP>`
<Application ShortName=*ShortName*> em que *ShortName* é o nome abreviado de um aplicativo especificado na seção "Applications".			

Tabela 12. (continuação)

Seção	Comando	Valor	O que ele faz
	<Name>	Uma cadeia de texto.	Especifica o nome do aplicativo.
	<Version>	Um valor numérico.	Especifica a versão do aplicativo.

	<Detects>
	
	<Detect>
		Root, PathAndKey	Especifica uma chave de registro. O SMA detecta um aplicativo procurando pela chave de registro especificada.
			
			Por exemplo,
			`<Detects>`
			`<Detect>`
			`<hive>HKLM</hive>`
			`<keyname>Software\Adobe\Acrobat Reader\5.0\</keyname>`
			`</Detect>`
			`</Detects>`

<Install_Directories>
 	
Por exemplo:
`<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>`
`<Regsitry>`
`<hive>HKLM</hive>`
`<keyname>Software\adobe\Acrobat Reader\5.0\InstallPath</keyname>`
`<value>(Default)</value>`
`</Registry>`
`</Install_Directory>`
`</Install_Directories>`			

	<OS>	Uma cadeia de texto.	O S.O. especifica o sistema operacional e pode ser um dos seguintes: • WinXP • Win2000 • WinNT • Win98
	<Registry>	*hive* é HKLM ou HKCU. *keyname* é o nome da chave. *value* é um comando opcional que especifica o valor do registro que é migrado.	Especifica o diretório de instalação como ele aparece no registro.
<Files_From_Folders> Opcional			

Tabela 12. (continuação)

Seção	Comando	Valor	O que ele faz

	SMAVariable\Location[|File][/s]
	
	em que
	• SMAvariable é uma das seguintes variáveis que especificam o local dos arquivos de customização:
	– %Windows Directory% (local de arquivos do sistema operacional).
	– %Install Directory% (local do aplicativo, conforme definido na seção Install_Directories).
	– %Appdata Directory% (o diretório de Dados do Aplicativo, que é um subdiretório do diretório de perfil do usuário).
	– %LocalAppdata Directory% (o diretório de Dados do Aplicativo na pasta Configurações Locais, que é um subdiretório do diretório de perfil do usuário).
	– %Cookies Directory% (o diretório de Cookies, que é um subdiretório do diretório de perfil do usuário).
	– %Favorites Directory% (o diretório de Favoritos, que é um subdiretório do diretório de perfil do usuário).
	– %%Personal Directory% (o diretório Pessoal, que é um subdiretório (Meus Documentos) do diretório de perfil do usuário. Esta variável de ambiente não pode ser utilizada pelo Windows NT4).
			Especifica os arquivos de customização que você deseja migrar.
			
			Por exemplo:
			`<Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi</Files_And_Folders>`
			
			O SMA captura os arquivos na pasta %AppData Directory%\Adobe\Acrobat\Whapi.
			
			pi. Os arquivos dos subdiretórios não são incluídos.
			`<Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi\ /s</Files_From_Folder>`
			
			O SMA captura os arquivos na pasta %AppData Directory%\Adobe\Acrobat\Whapi. Os arquivos dos subdiretórios são incluídos.
			`<Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi\*.*</Files_From_Folder>`
			
			O SMA captura os arquivos na pasta %AppData Directory%\Adobe\Acrobat\Whapi. Os arquivos dos subdiretórios não são incluídos.
			`<Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi\*.* /s</Files_From_Folder>`
			
			O SMA captura os arquivos na pasta %AppData Directory%\Adobe\Acrobat\Whapi. Os arquivos dos subdiretórios são incluídos.
			`<Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi</Files_From_Folder>`
			
			Quando "\" não segue o "Whapi", o SMA trata o "Whapi" não como uma pasta, mas como um arquivo.

Tabela 12. (continuação)

Seção	Comando	Valor	O que ele faz
	• *Location* especifica um arquivo ou diretório completo. Você pode utilizar caracteres curinga no nome do arquivo, mas não no caminho. Se você especificar um diretório, todos os arquivos serão copiados. • *[File]* é um parâmetro opcional que poderá ser utilizado apenas se Location especificar um diretório e File for o arquivo a ser copiado. Você pode utilizar caracteres curinga no nome do arquivo, mas não no caminho. • *[\s]* é um parâmetro opcional. Se você utilizar [/s], todos os arquivos dos subdiretórios serão copiados. • O usuário do SMA5.0 pode utilizar a variável de ambiente do Windows. A variável de ambiente do usuário que iniciou o SMA é utilizada como o valor de uma variável de ambiente do Windows.		
<Registries> Opcional			

	hive é HKLM ou HKCU.
	
	keyname é o nome da chave. Value é um comando opcional que especifica o valor do registro que é migrado.
			Especifica as entradas de registro que você deseja migrar.
			
			Por exemplo:
			`<Registries>`
			`<Registry>`
			`<hive>HKCU</hive>`
			`<keyname>Software\Adobe\Acrobat</keyname>`
			`<value></value>`
			`</Registry>`
			`</Registries>`

<Registry_Excludes> Opcional			

	hive é HKLM ou HKCU.
	
	keyname é o nome da chave. Value é um comando opcional que especifica o valor do registro que é migrado.
			Especifica as chaves de registro e os valores que você deseja excluir das entradas de registro selecionadas.
			
			Por exemplo:
			`<Registry_Excludes>`
			`<Registry>`
			`<hive>HKCU</hive>`
			`<keyname>Software\Adobe\Acrobat Reader\5.0\AdobeViewer`
			`</keyname>`
			`<value>xRes</value>`
			`</Registry>`
			`</Registry_Excludes>`

<Files_Through_Registry>			

Tabela 12. (continuação)

Seção	Comando	Valor	O que ele faz
	<OS> especifica o sistema operacional e é um dos seguintes valores: • WinXP • Win2000 • WinNT • Win98 <Registry> especifica a entrada de registro e está no formato hive,keyname,value, em que: • hive é HKLM ou HKCU. • keyname é o nome da chave. • Value é um comando opcional que especifica o valor do registro que é migrado. File é o nome do arquivo. Você pode utilizar caracteres curinga. File é o nome do arquivo. Você pode utilizar caracteres curinga.		Especifica os arquivos de customização a serem migrados. Por exemplo: <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> executa o processamento de batch antes do processamento de <Registries> por Aplicar. Por exemplo: <PreTargetBatchProcessing> <!CDATA[copy /y c:\temp*.* c:\migration del c:\migration*.mp3 </PreTargetBatchProcessing>
<TargetBatchProcessing>			
	<TargetBatchProcessing> <!CDAT[batch commands]] <TargetBatchProcessing>		<TargetBatchProcessing> executa o processamento de batch depois do processamento de <Registries> por Aplicar. Por exemplo: <TargetBatchProcessing> <!CDATA[copy /y c:\temp*.* c:\migration del c:\migration*.mp3 <TargetBatchProcessing>

Criando um Arquivo de Aplicativo

Para determinar quais configurações de aplicativo devem ser migradas para arquivos de aplicativos customizados, você deve testar cuidadosamente os aplicativos.

Conclua as etapas a seguir para criar um arquivo de aplicativo:

1. Utilize um editor de texto ASCII para abrir um arquivo application.XML existente. Se você instalou o SMA no local padrão, os arquivos application.XML estarão localizados no diretório d:\d:\%RR%\Migration\bin\Apps, em que d é a letra da unidade de disco rígido.

2. Modifique este arquivo application.XML para o aplicativo ou as configurações de aplicativos que você deseja migrar.
3. Modifique as informações na seção <Applications>.
4. Modifique os comandos <Name> e <Version> na seção <Application Shortname=*Shortname*>.
5. Determine as chaves de registro que devem ser migradas:
   a. Clique em **Iniciar → Executar**. A janela "Executar" é exibida. No campo **Abrir**, digite regedit e clique em **OK**. A janela "Editor de Registros" é exibida.
   b. Na área de janela à esquerda, expanda o nó **HKEY_LOCAL_MACHINE**.
   c. Expanda o nó **Software**.
   d. Expanda o nó específico do fornecedor, por exemplo, **Adobe**.
   e. Continue a navegar até localizar a chave de registro do aplicativo. Neste exemplo, a chave de registro é SOFTWARE\Adobe\Acrobat Reader\6.0.
   f. Defina o valor do campo Detect. Por exemplo:

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

6. Modifique os comandos Name e Version na seção Install_Directories.
7. Determine o caminho para os diretórios de instalação do aplicativo.
   a. Na janela "Editor de Registros", navegue até o nó HKLM\SOFTWARE\Adobe\Acrobat Reader\6.0\InstallPath.
   b. Inclua o comando apropriado para a seção Install_Directories do arquivo de aplicativo. Por exemplo:

```
<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: Se você não localizar um diretório específico do aplicativo no diretório HKLM\Software\Microsoft\Windows\CurrentVersion\AppPaths, deverá localizar um diretório que contém o caminho de instalação em alguma outra parte da árvore HKLM\Software. Em seguida, utilize essa chave na seção <Install_Directories>.
8. Na seção <Files_From Folders>, especifique os arquivos de customização que você deseja migrar.
   a. Como, por padrão, vários aplicativos salvam arquivos no subdiretório Documentos e Configurações, selecione o diretório de dados Aplicativos para os diretórios que pertençam ao aplicativo. Se houver algum, você poderá utilizar o seguinte comando para migrar o diretório e os arquivos:

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

   em que Location/ é um arquivo ou diretório completo e [File] é um parâmetro opcional que poderá ser utilizado apenas se Location/ especificar um diretório. No exemplo do Adobe Reader, os arquivos de customização estão no diretório Preferências.

b. Selecione todos os diretórios relacionados das configurações pessoais que podem ser armazenadas lá.
c. Selecione o diretório Configurações Locais.

9. Determine as entradas de registro que você deseja migrar. Elas estarão em HKCU (HKEY_CURRENT_USER). Na seção <Registries> do arquivo de aplicativo, inclua os comandos apropriados.
10. Salve o arquivo application.XML no diretório d:\Program Files\ThinkVantage\SMA\Apps, em que d é a letra da unidade de disco rígido.
11. Teste o novo arquivo de aplicativo.

Exemplo de um Arquivo application.XML do Adobe Reader

Esta seção contém um arquivo de aplicativo do 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_Direcotry>
                <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 Readr 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>
```

Atualização do Sistema

Active Update

Para determinar se o Active Update Launcher está instalado, verifique a existência da seguinte chave de registro:

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

Para determinar se o Active Update Launcher está configurado para permitir Atualização Ativa, o TVT verifica dentro de sua própria chave de registro o valor do atributo EnableActiveUpdate. Se EnableActiveUpdate=1, o TVT incluirá o item de menu ActiveUpdate no menu Ajuda.

Para chamar uma Atualização Ativa, a chamada do TVT ativa o programa Active Update Launcher e transmite um arquivo de parâmetro.

Utilize as seguintes etapas para chamar o Active Update:

1. Abra a chave de registro do Active Update Launcher:
   ```
   HKLM\software\TVT\ActiveUpdate
   ```
2. Obtenha o valor do atributo Path.
3. Obtenha o valor do atributo Program.

Capítulo 6. Instalação

O Pacote de Instalação do Rescue and Recovery/Client Security Solution é desenvolvido com o InstallShield 10.5 Premier como um projeto MSI Básico. Os projetos MSI Básicos do InstallShield 10.5 utilizam o Windows Installer para instalar aplicativos, o que dá aos administradores muitos recursos para customizar as instalações, como configurar valores de propriedades na linha de comandos. As próximas seções descrevem maneiras de utilizar e executar o pacote de instalação do Rescue and Recovery 3.0. Para melhor compreensão, leia o capítulo inteiro antes de começar a instalar o pacote.

Nota: Ao instalar este pacote, consulte o arquivo Leia-me publicado na página da Web da Lenovo em:

www.Lenovo.com/ThinkVantage

O arquivo leia-me contém informações atualizadas sobre assuntos tais como versões de software, sistemas suportados, requisitos do sistema e outras considerações para ajuda no processo de instalação.

Requisitos de Instalação

Esta seção trata dos requisitos do sistema para instalar o pacote do Rescue and Recovery/Client Security Solution. Para melhores resultados, vá para o seguinte Web site para certificar-se de que você tenha a versão mais recente do software:

www.Lenovo.com/ThinkVantage

Vários computadores de legado da IBM podem suportar o Rescue and Recovery, desde que atendam aos requisitos especificados. Consulte a página de download na Web para obter informações sobre computadores da marca IBM que suportam o Rescue and Recovery.

Requisitos para Computadores das Marcas IBM e Lenovo

Os computadores das marcas IBM e Lenovo devem satisfazer ou exceder os seguintes requisitos para executar o Rescue and Recovery:

- Sistema operacional: Microsoft Windows XP ou Windows 2000
- Processador: Conforme especificado pela Microsoft para Windows XP (Home ou Professional) e Windows 2000
  - Service pack 1, no mínimo
- Memória: 128 MB
  - Em configurações de memória compartilhada, a configuração da BIOS para o máximo de memória compartilhada deverá ser definida como no mínimo 4 MB e no máximo 8 MB.
  - Em configurações de memória não compartilhada, 120 MB de memória não compartilhada.

    Nota: Se o computador tiver menos de 200 MB de memória não compartilhada, o Rescue and Recovery será executado. Entretanto, talvez o usuário não consiga iniciar mais de um aplicativo no ambiente do Rescue and Recovery.

- 1,5 GB de espaço livre no disco rígido (a instalação básica requer 930 MB e não inclui o espaço necessário para backups do Rescue and Recovery)
- Vídeo compatível com VGA que suporte uma resolução de 800 x 600 e 24 bits de cor.
- Placa Ethernet suportada.

Requisitos para Instalação e Uso em Computadores Não-IBM ou Não-Lenovo

A instalação em computadores não-IBM ou não-Lenovo tem os seguintes requisitos:

Requisitos de Instalação

1,5 GB de espaço livre no disco rígido. A instalação básica utiliza 930 MB.

Requisitos Mínimos de Memória do Sistema

O computador não-IBM ou não-Lenovo deve ter 128 MB de RAM no sistema para instalar o Rescue and Recovery.

Configuração da Unidade de Disco Rígido

O programa Rescue and Recovery não é suportado nos pré-carregamentos de fábrica em computadores OEM (fabricante de equipamentos originais) (não-IBM ou não-Lenovo). Nos computadores OEM, a unidade de disco rígido deve ser configurada de acordo com as recomendações descritas em "Instalando o Rescue and Recovery em Computadores Não-IBM" na página 124.

Adaptadores de Rede

O ambiente do Rescue and Recovery suporta apenas adaptadores de rede Ethernet, baseados em PCI com conexão física. Os drivers do dispositivo de rede incluídos no ambiente do Rescue and Recovery são os mesmos drivers que foram pré-populados no sistema operacional Microsoft Windows XP Professional e são independentes do sistema operacional Windows. Para computadores das marcas Lenovo e IBM suportados, os drivers necessários são incluídos com o software Rescue and Recovery.

Se um dispositivo de rede OEM em seu computador não for suportado, consulte a documentação fornecida com o dispositivo, a fim de obter instruções para incluir suporte aos drivers de rede específicos do sistema. Solicite os drivers ao seu OEM.

Suporte para Inicialização a Partir de Mídia Externa (CD/DVD e USB)

Computadores e dispositivos não-IBM/não-Lenovo (unidade de disco rígido USB, CD-R/RW, DVD-R/RW/RAM ou DVD+R/RW) devem suportar totalmente uma ou mais das seguintes especificações:

- Especificação da BIOS do Dispositivo de Mídia Removível ATAPI
- Serviços de Unidade de Disco Avançada da BIOS - 2
- Especificação de Inicialização da BIOS Compaq Phoenix Intel
- Especificação de Formato de CD-ROM Inicializável El Torito
- Visão Geral da Especificação de classe de armazenamento em Massa USB (cada dispositivo deve respeitar a especificação de bloco de comando no código de Subclasse da seção 2.0 na "Visão Geral da Especificação de classe de armazenamento em Massa USB").
- Especificação de Armazenamento em Massa USB para Inicialização

Requisitos de Vídeo

- **Compatibilidade do Vídeo:** Vídeo compatível com VGA que suporte uma resolução de 800 x 600 e 24 bits de cor.

- **Memória de Vídeo:**
  - Em sistemas de memória de vídeo não compartilhada: um mínimo de 4 MB de RAM de vídeo.
  - Em sistemas de memória de vídeo compartilhada: um mínimo de 4 MB e um máximo de 8 MB pode ser alocado para memória de vídeo.

Compatibilidade do Aplicativo

Alguns aplicativos que tenham ambientes de driver de filtro complexo (como software de antivírus) podem não ser compatíveis com o software do Rescue and Recovery. Para obter informações em relação a questões de compatibilidade, consulte o arquivo LEIA-ME que acompanha o software Rescue and Recovery na Web:

www.lenovo.com/ThinkVantage

Utilitários

Este guia refere-se a vários utilitários. Esses utilitários podem ser encontrados neste Web site:

www.Lenovo.com/ThinkVantage

Componentes de Instalação do Rescue and Recovery

1. Pacote de instalação principal (aproximadamente 45 MB): Este é o setup.exe construído a partir da origem do projeto de instalação. O arquivo setup.exe é renomeado durante o processo de construção para um nome que representa o ID do projeto, o tipo de mídia, o nível da construção, o código do país (sempre US neste caso) e o código de correção – por exemplo, Z096ZIS1001US00.exe. Este é um pacote de instalação de extração automática que extrai os arquivos de origem da instalação e ativa a instalação utilizando o Windows Installer. Ele contém a lógica de instalação e os arquivos do aplicativo do Windows. O pacote não contém nenhum dos arquivos de pré-desktop.
2. Base de pré-desktop em inglês (US) (aproximadamente 135 MB): Este é o arquivo zip protegido por senha que contém toda a base de pré-desktop US. Seu nome é no formato Z062ZAA1001US00.TVT, em que *AA* determina a compatibilidade do pré-desktop e *001* é o nível do pré-desktop. Este arquivo é necessário para instalar o pré-desktop nos sistemas de todos os idiomas. Este arquivo deve estar no mesmo diretório do pacote de instalação principal (setup.exe, ou Rescue and Recovery/Client Security Solution.msi se for extraído ou uma instalação de OEM). As exceções a isso são se o pré-desktop já estiver instalado e não precisar que seja feito upgrade, ou se a propriedade PDA=0 for configurada na linha de comando ao executar a instalação e o pré-desktop (qualquer versão) ainda não existir. O setup.exe contém um arquivo pdaversion.txt que contém a versão mínima do pré-desktop que pode funcionar com essa versão do Windows. O instalador setup.exe procurará um arquivo de pré-desktop usando a seguinte lógica:
   - **O Pré-desktop antigo (RNR 1.0 ou 2.X) existe ou nenhum Pré-desktop existe:**

     O instalador procurará um arquivo .TVT com um código de compatibilidade (por exemplo, AA, AB) que seja igual ao código de compatibilidade da versão mínima e um nível que seja maior que ou igual à versão mínima (todos os outros campos de versão no nome do arquivo .TVT devem corresponder exatamente à versão mínima). Se não for localizado um arquivo correspondente a esses critérios, a instalação será interrompida.
   - **O Novo (RNR 3.0) Pré-desktop existe:**

O instalador comparará o versão do pré-desktop atual com o código de compatibilidade da versão mínima e tomará as seguintes ações com base nos resultados:

- Código **atual > Código mínimo:**

  O instalador apresentará uma mensagem indicando que o ambiente atual não é compatível com esta versão do RNR.

- Código **atual = Código mínimo:**

  O instalador comparará o nível da versão atual com o nível da versão mínima. Se o nível atual for maior que ou igual ao nível mínimo, o instalador procurará um arquivo .TVT com um código de compatibilidade (AA, AB...) que seja igual ao código de compatibilidade da versão mínima e um nível que seja maior que o nível da versão atual (todos os outros campos de versão no nome do arquivo .TVT deverão corresponder exatamente à versão mínima). Se ele não localizar um arquivo, o processo de instalação continuará sem atualizar o pré-desktop. Se o nível atual for menor que o nível mínimo, o instalador procurará um arquivo .TVT com um código de compatibilidade (AA, AB...) que seja igual ao código de compatibilidade da versão mínima e um nível que seja maior que ou igual ao nível da versão mínima (todos os outros campos de versão no nome do arquivo .TVT deverão corresponder exatamente à versão mínima). Se não for localizado um arquivo correspondente a esses critérios, a instalação será interrompida.

- Código **atual > Código mínimo:**

  O instalador procurará um arquivo .TVT com um código de compatibilidade (AA, AB...) que seja igual ao código de compatibilidade da versão mínima e um nível que seja maior que ou igual à versão mínima (todos os outros campos de versão no nome do arquivo .TVT deverão corresponder exatamente à versão mínima). Se não for localizado um arquivo correspondente a esses critérios, a instalação será interrompida.

3. Pacotes de idioma do pré-desktop (aproximadamente 5 a 30 MB cada): Existem 24 pacotes de idioma para o Windows PE que são suportados no Rescue and Recovery 3.0. O nome de cada pacote de idioma tem o formato Z062ZAA1001CC00.TVT em que o CC representa o idioma. Um desses arquivos é necessário se o pré-desktop estiver sendo instalado em um sistema que não seja em inglês ou em um sistema com um idioma não suportado e deve estar no mesmo diretório da instalação principal e do arquivo .TVT do pré-desktop em inglês (US). O idioma do pacote de idioma deve corresponder ao idioma do Windows se o Windows não for em inglês ou for em um idioma não suportado pelos pacotes de idioma. Se o pré-desktop estiver sendo instalado ou atualizado e um pacote de idioma for necessário, a instalação procurará um pacote de idioma .TVT em que todos os campos no nome do arquivo correspondam ao nome do arquivo de pré-desktop em inglês (US) exceto pelo código do idioma, o qual deve corresponder ao idioma do sistema. Os pacote des idioma estão disponíveis nos seguinte idiomas:
   - Árabe
   - Português do Brasil
   - Português
   - Tcheco
   - Dinamarquês
   - Finlandês
   - Francês

- Grego
- Alemão
- Hebraico
- Hong Kong
- Chinês
- Húngaro
- Italiano
- Japonês
- Coreano
- Holandês
- Norueguês
- Polonês
- Português
- Russo
- Chinês Simplificado
- Espanhol
- Sueco
- Chinês Tradicional
- Turco

Procedimento de Instalação Padrão e Parâmetros da Linha de Comandos

O setup.exe pode aceitar um conjunto de parâmetros de linha de comandos, os quais são descritos a seguir. As opções da linha de comandos que exigirem um parâmetro deverão ser especificadas sem espaço entre a opção e seu parâmetro. Por exemplo, Setup.exe /s /v"/qn REBOOT="R"" é válido, enquanto Setup.exe /s /v "/qn REBOOT="R"" não é. Aspas delimitando um parâmetro de opção são necessárias somente se o parâmetro contiver espaços.

Nota: O comportamento padrão da instalação quando executadas sozinha (executando apenas setup.exe sem nenhum parâmetro) é avisar o usuário para reinicializar no final da instalação. É necessária uma reinicialização para que o programa funcione corretamente. A reinicialização pode ser retardada através de um parâmetro da linha de comandos para uma instalação silenciosa conforme documentado acima e na seção de exemplos.

Os parâmetros e descrições a seguir foram extraídos diretamente da documentação de ajuda a desenvolvedores do InstallShield. Os parâmetros que não se aplicam a projetos MSI Básicos foram removidos.

Tabela 13.

Parâmetro	Descrição
/a : Instalação administrativa	A chave /a faz com que o Setup.exe execute uma instalação administrativa. Uma instalação administrativa copia (e descompacta) os arquivos de dados para um diretório especificado pelo usuário, mas não cria atalhos, registra servidores COM ou cria um registro de desinstalação.

Tabela 13. (continuação)

Parâmetro	Descrição
/x : Modo de desinstalação	A chave /x faz com que o Setup.exe desinstale um produto instalado anteriormente.
/s : Modo silencioso	O comando Setup.exe /s suprime a janela de inicialização do Setup.exe para um programa de instalação MSI Básico, mas não lê um arquivo de resposta. Os projetos MSI Básicos não criam nem utilizam um arquivo de resposta para instalações silenciosas. Para executar um produto MSI Básico silenciosamente, execute Setup.exe /s /v/qn na linha de comandos. (Para especificar os valores de propriedades públicas para uma instalação MSI Básica silenciosa, é possível utilizar um comando como Setup.exe /s /v"/qn INSTALLDIR=D:\Destino").
/v : transmitir argumentos para Msiexec	O argumento /v é utilizado para transmitir chaves da linha de comandos e valores de propriedades públicas para Msiexec.exe.
/L : Idioma de configuração	Os usuários podem utilizar a chave /L com o ID de idioma decimal para especificar o idioma utilizado por uma programa de instalação multi-idiomas. Por exemplo, o comando para especificar o idioma alemão é Setup.exe /L1031. Nota: Nem todos os idiomas relacionados na Tabela 14 são suportados na instalação.
/w : Aguardar	Para um projeto MSI Básico, o argumento /w força Setup.exe a aguardar até que a instalação esteja concluída antes de sair. Se você estiver utilizando a opção /w em um arquivo em batch, pode ser útil preceder todo o argumento da linha de comandos de Setup.exe com start /WAIT. Um exemplo corretamente formatado desse uso é o seguinte: `start /WAIT setup.exe /w`

Tabela 14.

Idioma	Identificador
Árabe (Arábia Saudita)	1025
Basco	1069
Búlgaro	1026
Catalão	1027
Chinês Simplificado	2052
Chinês Tradicional	1028
Croata	1050
Tcheco	1029
Dinamarquês	1030
Holandês (Padrão)	1043

Tabela 14. (continuação)

Idioma	Identificador
Inglês	1033
Finlandês	1035
Francês Canadense	3084
Francês	1036
Alemão	1031
Grego	1032
Hebraico	1037
Húngaro	1038
Indonésio	1057
Italiano	1040
Japonês	1041
Coreano	1042
Norueguês (Bokmal)	1044
Polonês	1045
Português do Brasil	1046
Português Padrão	2070
Romeno	1048
Russo	1049
Eslovaco	1051
Esloveno	1060
Espanhol	1034
Sueco	1053
Tai	1054
Turco	1055

Procedimento de Instalação Administrativa e Parâmetros de Linha de Comandos

O Windows Installer pode executar uma instalação administrativa de um aplicativo ou produto em uma rede para ser utilizado por um grupo de trabalho ou para personalização. No pacote de instalação do Rescue and Recovery/Client Security Solution, uma instalação administrativa desempacota os arquivos de origem da instalação em um local específico. Para executar uma instalação administrativa, o pacote de instalação precisa ser executado a partir da linha de comandos utilizando o parâmetro /a:

```
Setup.exe /a
```

A ativação de uma instalação administrativa apresenta uma séria de telas de diálogo que solicitam ao usuário administrativo para especificar o local para descompactar os arquivos de instalação. O local de extração padrão apresentado ao usuário administrativo é C:\. Pode ser escolhido um novo local, o qual pode incluir unidades diferentes de C: (tais como outras unidades locais e unidades de rede mapeadas). Também é possível criar novos diretórios durante esta etapa.

Se uma instalação administrativa for executada silenciosamente, a propriedade pública TARGETDIR pode ser definida na linha de comandos para especificar o local de extração:

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

Após a conclusão de uma instalação administrativa, o usuário administrativo pode fazer customizações nos arquivos de origem, tais como incluir configurações adicionais em tvt.txt. Para instalar a partir da origem descompactada depois de fazer customizações, o usuário deve chamar msiexec.exe da linha de comandos, transmitindo o nome do arquivo msi descompactado.

A seção a seguir descreve os parâmetros de linha de comandos disponíveis que podem ser utilizados com msiexec, bem como exemplos de como utilizá-los. As propriedades públicas também podem ser configuradas diretamente na chamada a msiexec na linha de comandos.

Parâmetros de Linha de Comandos de MsiExec.exe

MsiExec.exe é o programa executável do Windows Installer utilizado para interpretar os pacotes de instalação e instalar produtos em sistemas de destino.

```
msiexec. /i "C:WindowsFolder/Profiles\UserName\Persona\MySetups\nome do projeto\
configuração do produto\nome do release\DiskImages\Disk1\nome do produto.msi
```

A tabela a seguir fornece uma descrição detalhada dos parâmetros de linha de comandos de MsiExec.exe. Essa tabela foi extraída diretamente da documentação do SDK da Plataforma Microsoft no Windows Installer.

Tabela 15.

Parâmetro	Descrição
/i *pacote* ou *código do produto*	Utilize este formato para formato o produto Othello: `msiexec /i "C:\WindowsFolder\Profiles\ UserName\Personal\MySetups\Othello\Trial Version\ Release\DiskImages\Disk1\Othello Beta.msi"` Código do Produto refere-se ao GUID que é gerado automaticamente na propriedade de Código do Produto na visualização do projeto de seu produto.

Tabela 15. (continuação)

Parâmetro	Descrição
/f [p|o|e|d|c|a|u|m|s|v] *pacote* ou *código do produto*	A instalação com a opção /f reparará ou reinstalará arquivos ausentes ou corrompidos. Por exemplo, para forçar uma reinstalação de todos os arquivos, utilize a seguinte sintaxe: `msiexec /fa "C:\WindowsFolder\Profiles\ UserName\Personal\MySetups\Othello\Trial Version\ Release\DiskImages\Disk1\Othello Beta.msi"` em conjunto com os seguintes sinalizadores: • p reinstala um arquivo se ele estiver ausente. • o reinstala um arquivo se ele estiver ausente ou se um versão mais antiga do arquivo estiver presente no sistema do usuário. • e reinstala um arquivo se ele estiver ausente ou se uma versão equivalente ou mais antiga do arquivo estiver presente no sistema do usuário. • c reinstala um arquivo se ele estiver ausente ou se o checksum armazenado do arquivo instalado não corresponder ao valor do novo arquivo. • a força uma reinstalação de todos os arquivos. • u ou m recria todas as entradas necessárias no registro do usuário. • s sobrescreve quaisquer atalhos existentes. • v executa o aplicativo a partir da origem e rearmazena em cache o pacote de instalação local.
/a *pacote*	A opção /a permite a usuários com privilégios de administrador instalar um produto na rede.
/x *pacote* ou *código do produto*	A opção /x desinstala um produto.
/L [i|w|e|a|r |u|c|m|p|v|+] *arquivo de log*	A construção com a opção /L especifica o caminho para o arquivo de registro—esses sinalizadores indicam quais informações devem ser gravadas no arquivo de registro: • i registra mensagens de status. • w registra mensagens de aviso não fatais. • e registra todas as mensagens de erro. • a registra o início de seqüências de ações. • r registra registros específicos da ação. • u registra pedidos do usuário. • c registra parâmetros iniciais da interface com o usuário. • m registra mensagens de falta de memória. • p registra configurações do terminal. • v registra a configuração de saída detalhada. • + anexa a um arquivo existente. • * é um caractere curinga que permite registrar todas as informações (excluindo a configuração de saída detalhada).

Tabela 15. (continuação)

Parâmetro	Descrição
/q [n|b|r|f]	A opção /q é utilizada para configurar o nível da interface com o usuário em conjunto com os seguintes sinalizadores: • q ou qn não cria uma interface com o usuário. • qb cria uma interface com o usuário básica. As configurações de interface com o usuário a seguir exibem uma caixa de diálogo modal no final da instalação: • qr exibe uma interface com o usuário reduzida. • qf exibe uma interface com o usuário completa. • qn+ não exibe uma interface com o usuário. • qb+ exibe uma interface com o usuário básica.
/? ou /h	Qualquer um dos comandos exibe informações de copyright do Windows Installer.
TRANSFORMS	Utilize o parâmetro de linha de comando TRANSFORMS para especificar quaisquer transformações que você gostaria de aplicar em seu pacote básico. A chamada da linha de comandos de transformação pode se assemelhar a esta: `msiexec /i "C:\WindowsFolder\Profiles\UserName\Personal\MySetups\Your Project Name\Trial Version\My Release-1\DiskImages\Disk1\ProductName.msi" TRANSFORMS="New Transform 1.mst"` Você pode separar várias transformações com um ponto-e-vírgula. Portanto, recomenda-se não utilizar ponto-e-vírgula no nome da transformação, pois o serviço do Windows Installer os interpretará de maneira incorreta.
Propriedades	Todas as propriedades públicas podem ser definidas ou modificadas a partir da linha de comandos. As propriedades públicas se distinguem das propriedades privadas por estarem em letras maiúsculas. Por exemplo, COMPANYNAME é uma propriedade pública. Para configurar uma propriedade a partir da linha de comandos, utilize a seguinte sintaxe: PROPERTY=VALUE. Se você quisesse alterar o valor para COMPANYNAME, deveria digitar: `msiexec /i "C:\WindowsFolder\Profiles\UserName\Personal\MySetups\Your Project Name\Trial Version\My Release-1\DiskImages\Disk1\ProductName.msi" COMPANYNAME="InstallShield"`

Propriedades Públicas Padrão do Windows Installer

O Windows Installer tem um conjunto de propriedades públicas padrão incorporadas que podem ser configuradas na linha de comandos para especificar um determinado comportamento durante a instalação. As propriedades públicas mais comuns utilizadas na linha de comandos são descritas a seguir. Mais documentação está disponível no Web site da Microsoft em: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/about_properties.asp

A Tabela 16 na página 87 mostra as propriedades do Windows Installer comumente utilizadas:

Tabela 16.

Propriedade	Descrição
TARGETDIR	Especifica o diretório de destino raiz para a instalação. Durante uma instalação administrativa esta propriedade é o local para copiar o pacote de instalação.
ARPAUTHORIZEDCDFPREFIX	URL do canal de atualização para o aplicativo.
ARPCOMMENTS	Fornece Comentários para Adicionar ou remover programas no Painel de controle.
ARPCONTACT	Fornece Contato para Adicionar ou remover programas no Painel de controle.
ARPINSTALLLOCATION	Caminho completo para a pasta primária do aplicativo.
ARPNOMODIFY	Desativa a funcionalidade que modificaria o produto.
ARPNOREMOVE	Desativa a funcionalidade que removeria o produto.
ARPNOREPAIR	Desativa o botão Reparar no assistente de Programas.
ARPPRODUCTICON	Especifica o ícone primário do pacote de instalação.
ARPREADME	Fornece um Leia-me para Adicionar ou remover programas no Painel de controle.
ARPSIZE	Tamanho estimado do aplicativo em kilobytes.
ARPSYSTEMCOMPONENT	Impede a exibição do aplicativo na lista Adicionar ou remover programas.
ARPURLINFOABOUT	URL para a home page de um aplicativo.
ARPURLUPDATEINFO	URL para informações de atualização do aplicativo.
REBOOT	A propriedade REBOOT suprime certos avisos para uma reinicialização do sistema Um administrador geralmente utiliza esta propriedade com uma série de instalações para instalar vários produtos ao mesmo tempo com somente uma reinicialização no final. Configure REBOOT=″R″ para desativar quaisquer reinicializações no final de uma instalação.
INSTALLDIR	Esta propriedade contém a pasta de destino padrão para os arquivos dos recursos e componentes.

Propriedades Públicas Customizadas do Rescue and Recovery

O pacote de instalação do programa Rescue and Recovery contém um conjunto de propriedades públicas customizadas que podem ser das na linha de comandos ao executar a instalação. As propriedades públicas customizadas disponíveis são:

Tabela 17.

Propriedade	Descrição
PDA	Especifica se o pré-desktop deve ser instalado, o valor padrão é 1. 1 = instalar o pré-desktop, 0 = não instalar o pré-desktop. NOTA: esta configuração não é utilizada se já existir alguma versão do pré-desktop.
CIMPROVIDER	Especifica se o componente Provedor CIM deve ser instalado. O padrão é não instalar o componente. Especifique CIMPROIVIDER=1 na linha de comandos para instalar o componente.
EMULATIONMODE	Especifica que a instalação deve ser forçada no modo de Emulação mesmo se um TPM existir. Configure EMULATIONMODE=1 na linha de comandos para instalar no modo de Emulação.
HALTIFCSS54X	Se o CSS 5.4X estiver instalado e a instalação estiver executando no modo silencioso, o padrão é que a instalação prossiga no modo de emulação. Utilize a propriedade HALTIFCSS54X=1 ao executar a instalação no modo silencioso para interromper a instalação se o CSS 5.4X estiver instalado.
HALTIFTPMDISABLED	Se o TPM estiver em um estado desativado e a instalação estiver executando no modo silencioso, o padrão é que a instalação prossiga no modo de emulação. Utilize a propriedade HALTIFTPMDISABLED=1 ao executar a instalação no modo silencioso para interromper a instalação se o TPM estiver desativado.
ENABLETPM	Configure ENABLETPM=0 na linha de comandos para impedir que a instalação ative o TPM.
NOCSS	Configure NOCSS=1 na linha de comandos para impedir que o Client Security Solution e seus subrecursos sejam instalados. Isto é destinado a ser utilizado com uma instalação silenciosa mas pode ser utilizado também com uma instalação de UI. Na instalação de UI, o recurso CSS não será mostrado na tela de configuração customizada.
NOPRVDISK	Configure NOPRVDISK=1 na linha de comandos para impedir que o recurso PrivateDisk do SafeGuard seja instalado. Isto é destinado a ser utilizado com uma instalação silenciosa mas pode ser utilizado também com uma instalação de UI. Na instalação de UI, o recurso PrivateDisk do SafeGuard não será mostrado na tela de configuração customizada.

Tabela 17. (continuação)

Propriedade	Descrição
NOPWMANAGER	Configure NOPWMANAGER=1 na linha de comandos para impedir que o recurso Password Manager seja instalado. Isto é destinado a ser utilizado com uma instalação silenciosa mas pode ser utilizado também com uma instalação de UI. Na instalação de UI, o recurso Password Manager não será mostrado na tela de configuração customizada.
NOCSSWIZARD	Configure NOCSSWIZARD=1 na linha de comandos para impedir que o Assistente CSS seja exibido quando um usuário administrativo efetuar logon e não tiver sido inscrito. Esta propriedade é destinada a alguém que deseje instalar o CSS mas utilizar scripts posteriormente para realmente configurar o sistema.
CSS_CONFIG_SCRIPT	Configure CSS_CONFIG_SCRIPT="*nome_do_arquivo*" ou "*nome_do_arquivo senha*" para fazer com que um arquivo de configuração seja executado depois que o usuário concluir a instalação e reinicializar.
SUPERVISORPW	Configure SUPERVISORPW="*senha*" na linha de comandos para fornecer a senha do supervisor para ativar o chip no modo de instalação silencioso ou não silencioso. Se o chip estiver desativado e a instalação estiver executando no modo silencioso, a senha correta do supervisor deve ser fornecida para ativar o chip, caso contrário o chip não será ativado.

Arquivo de Registro da Instalação

Um arquivo de registro rrinstall30.log será criado no diretório %temp% se a instalação for ativada por setup.exe (dando um clique duplo no exe principal de instalação, executando o exe principal sem parâmetros ou extraindo o msi e executando setup.exe). Esse arquivo contém mensagens de registro que podem ser utilizadas para depurar problemas de instalação. Esse arquivo de registro não será criado ao executar o setup diretamente do pacote msi; isso inclui quaisquer ações executadas a partir de Adicionar ou remover programas. Para criar um arquivo de registro para todas as ações de MSI, você pode ativar a política de registro em log no registro. Para isso, crie o valor:

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

Exemplos de Instalação

A tabela a seguir mostra exemplos utilizando setup.exe:

Tabela 18.

Descrição	Exemplo
Instalação Silenciosa sem Reinicialização	`setup.exe /s /v"/qn REBOOT="R""`

Tabela 18. (continuação)

Descrição	Exemplo
Instalação Administrativa	`setup.exe /a`
Instalação Administrativa Silenciosa especificando o local de extração	`setup.exe /a /s /v"/qn TARGETDIR="F:\TVTRR""`
Desinstalação Silenciosa setup.exe /s /x /v/qn	`setup.exe /s /x /v/qn`
Instalação sem Reinicialização e criação de um registro de instalação no diretório temp	`setup.exe /v"REBOOT="R" /L*v %temp%\rrinstall30.log"`
Instalação sem instalar o pré-desktop setup.exe /vPDA=0	`setup.exe /vPDA=0`

A tabela a seguir mostra exemplos de instalação utilizando o Solution.msi do Rescue and Recovery/Client:

Tabela 19.

Descrição	Exemplo
Instalar	msiexec /i "C:\TVTRR\Rescue and Recovery/Client Security Solution.msi"
Instalação Silenciosa sem Reinicialização	msiexec /i "C:\TVTRR\Rescue and Recovery/Client Security Solution.msi" /qn REBOOT="R"
Desinstalação Silenciosa	msiexec /x "C:\TVTRR\Rescue and Recovery/Client Security Solution.msi" /qn
Instalação sem instalar o pré-desktop	msiexec /i "C:\TVTRR\Rescue and Recovery/Client Security Solution.msi" PDA=0

Incluindo o Rescue and Recovery em uma Imagem de Disco

Você pode utilizar a ferramenta de sua preferência para criar uma imagem de disco que inclua o Rescue and Recovery. Esse guia de implementação fornece informações básicas a respeito do PowerQuest e do Ghost, à medida que eles se aplicam a este aplicativo e a esta instalação. Supõe-se que você tenha experiência em sua ferramenta de criação de imagens e que incluirá outras opções necessárias em seus aplicativos.

Nota: Se você planeja criar uma imagem, deverá capturar o Registro de Inicialização Principal. O Registro de Inicialização Principal é crítico para que o ambiente do Rescue and Recovery funcione corretamente.

Utilizando Ferramentas Baseadas na Imagem da Unidade PowerQuest

Supondo-se que o PQIMGCTR da ferramenta PowerQuest DeployCenter esteja instalado no seguinte local (X:\PQ), você poderá criar e implementar uma imagem com o Rescue and Recovery com os seguintes scripts:

Mínimo de Scripts de Arquivos

Tabela 20. X:\PQ\RRUSAVE.TXT

Idioma do Script	Resultado
`SELECT DRIVE 1`	Selecionar primeira unidade de disco rígido

Tabela 20. X:\PQ\RRUSAVE.TXT (continuação)

Idioma do Script	Resultado
SELECT PARTITION ALL (Necessário se você tiver uma partição tipo 12 ou se tiver várias partições em sua imagem).	Selecionar todas as partições
Armazenar com compactação alta	Armazenar a imagem

Tabela 21. X:\PQ\RRDEPLY.TXT

Idioma do Script	Resultado
SELECT DRIVE 1	Selecionar primeira unidade de disco rígido
DELETE ALL	Excluir todas as partições
SELECT FREESPACE FIRST	Selecionar primeiro espaço livre
SELECT IMAGE ALL	Selecionar todas as partições na imagem
RESTORE	Restaurar a imagem

Criação de Imagem

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

Idioma do Script	Resultado
SELECT DRIVE 1	Selecionar primeira unidade de disco rígido
X:\PQ\PQIMGCTR	Programa de imagens
/CMD=X:\PQ\RRUSAVE.TXT	Script de arquivo PowerQuest
/MBI=1	Capturar o Gerenciador de Reinicialização do Rescue and Recovery
/IMG=X:\IMAGE.PQI	Arquivo de imagem

Implementação de Imagem

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

Idioma do Script	Resultado
SELECT DRIVE 1	Selecionar primeira unidade de disco rígido
X:\PQ\PQIMGCTR	Programa de imagens
/CMD=X:\PQ\RRDEPLY.TXT	Script de arquivo PowerQuest
/MBR=1	Restaurar o Gerenciador de Reinicialização do Rescue and Recovery
/IMG=X:\IMAGE.PQI	Arquivo de imagem

Utilizando Ferramentas Baseadas no Symantec Ghost

Quando você criar a imagem Ghost, deverá utilizar o comutador da linha de comandos (que pode estar incorporado no arquivo GHOST.INI) `-ib` para capturar o Gerenciador de Reinicialização do Rescue and Recovery. Além disso, a imagem deverá capturar o disco inteiro e todas as partições. Consulte a documentação fornecida pela Symantec para obter detalhes específicos sobre o Ghost.

Componentes de Instalação do Client Security Solution Versão 6.0

O Pacote de Instalação do Client Security Solution 6.0 é desenvolvido com o InstallShield 10.5 Premier como um projeto MSI Básico. Os projetos MSI Básicos do InstallShield 10.5 utilizam o Windows Installer para instalar aplicativos, o que dá aos administradores muitos recursos para customizar as instalações, como configurar valores de propriedades na linha de comandos. As seções a seguir descrevem maneiras de utilizar e executar o pacote de instalação do CSS 6.0. Para uma melhor compreensão, leia todas as instruções a seguir.

Componentes da Instalação

A Instalação do CSS 6.0 consiste em um único arquivo exe (aproximadamente 20 MB). Este é o setup.exe construído a partir da origem do projeto de instalação. O arquivo setup.exe é renomeado durante o processo de construção para um nome que representa o ID do projeto, o tipo de mídia, o nível da construção, o código do país (sempre US neste caso) e o código de correção – por exemplo, 169ZIS1001US00.exe. Este é um pacote de instalação de extração automática que extrai os arquivos de origem da instalação e ativa a instalação utilizando o Windows Installer. Ele contém a lógica de instalação e os arquivos do aplicativo do Windows.

Procedimento de Instalação Padrão e Parâmetros da Linha de Comandos

O setup.exe pode aceitar um conjunto de parâmetros de linha de comandos, os quais são descritos a seguir. As opções da linha de comandos que exigirem um parâmetro deverão ser especificadas sem espaço entre a opção e seu parâmetro. Por exemplo,

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

é válido, enquanto

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

não é. Aspas delimitando um parâmetro de opção são necessárias somente se o parâmetro contiver espaços.

Nota: O comportamento padrão da instalação quando executadas sozinha (executando apenas setup.exe sem nenhum parâmetro) é avisar o usuário para reinicializar no final da instalação. É necessária uma reinicialização para que o programa funcione corretamente. A reinicialização pode ser retardada através de um parâmetro da linha de comandos para uma instalação silenciosa conforme documentado acima e na seção de exemplos.

Os parâmetros e descrições a seguir foram extraídos diretamente da documentação de ajuda a desenvolvedores do InstallShield. Os parâmetros que não se aplicam a projetos MSI Básicos foram removidos.

Tabela 24.

Parâmetro	Descrição
/a : Instalação administrativa	A chave /a faz com que o Setup.exe execute uma instalação administrativa. Uma instalação administrativa copia (e descompacta) os arquivos de dados para um diretório especificado pelo usuário, mas não cria atalhos, registra servidores COM ou cria um registro de desinstalação.
/x : Modo de desinstalação	A chave /x faz com que o Setup.exe desinstale um produto instalado anteriormente.
/s : Modo silencioso	O comando Setup.exe /s suprime a janela de inicialização do Setup.exe para um programa de instalação MSI Básico, mas não lê um arquivo de resposta. Os projetos MSI Básicos não criam nem utilizam um arquivo de resposta para instalações silenciosas. Para executar um produto MSI Básico silenciosamente, execute Setup.exe /s /v/qn na linha de comandos. (Para especificar os valores de propriedades públicas para uma instalação MSI Básica silenciosa, é possível utilizar um comando como Setup.exe /s /v"/qn INSTALLDIR=D:\Destino").
/v : transmitir argumentos para Msiexec	O argumento /v é utilizado para transmitir chaves da linha de comandos e valores de propriedades públicas para Msiexec.exe.
/L : Idioma de configuração	Os usuários podem utilizar a chave /L com o ID de idioma decimal para especificar o idioma utilizado por uma programa de instalação multi-idiomas. Por exemplo, o comando para especificar o idioma alemão é Setup.exe /L1031. Nota: Nem todos os idiomas relacionados na Tabela 25 são suportados na instalação.
/w : Aguardar	Para um projeto MSI Básico, o argumento /w força Setup.exe a aguardar até que a instalação esteja concluída antes de sair. Se você estiver utilizando a opção /w em um arquivo em batch, pode ser útil preceder todo o argumento da linha de comandos de Setup.exe com start /WAIT. Um exemplo corretamente formatado desse uso é o seguinte: `start /WAIT setup.exe /w`

Tabela 25.

Idioma	Identificador
Árabe (Arábia Saudita)	1025
Basco	1069
Búlgaro	1026
Catalão	1027
Chinês Simplificado	2052

Tabela 25. (continuação)

Idioma	Identificador
Chinês Tradicional	1028
Croata	1050
Tcheco	1029
Dinamarquês	1030
Holandês (Padrão)	1043
Inglês	1033
Finlandês	1035
Francês Canadense	3084
Francês	1036
Alemão	1031
Grego	1032
Hebraico	1037
Húngaro	1038
Indonésio	1057
Italiano	1040
Japonês	1041
Coreano	1042
Norueguês (Bokmal)	1044
Polonês	1045
Português do Brasil	1046
Português Padrão	2070
Romeno	1048
Russo	1049
Eslovaco	1051
Esloveno	1060
Espanhol	1034
Sueco	1053
Tai	1054
Turco	1055

Procedimento de Instalação Administrativa e Parâmetros de Linha de Comandos

O Windows Installer pode executar uma instalação administrativa de um aplicativo ou produto em uma rede para ser utilizado por um grupo de trabalho ou para personalização. No pacote de instalação do Rescue and Recovery/Client Security Solution, uma instalação administrativa desempacota os arquivos de origem da instalação em um local específico. Para executar uma instalação administrativa, o pacote de instalação precisa ser executado a partir da linha de comandos utilizando o parâmetro /a:

```
Setup.exe /a
```

A ativação de uma instalação administrativa apresenta uma séria de telas de diálogo que solicitam ao usuário administrativo para especificar o local para descompactar os arquivos de instalação. O local de extração padrão apresentado ao usuário administrativo é C:\. Pode ser escolhido um novo local, o qual pode incluir unidades diferentes de C: (tais como outras unidades locais e unidades de rede mapeadas). Também é possível criar novos diretórios durante esta etapa.

Se uma instalação administrativa for executada silenciosamente, a propriedade pública TARGETDIR pode ser definida na linha de comandos para especificar o local de extração:

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

Após a conclusão de uma instalação administrativa, o usuário administrativo pode fazer customizações nos arquivos de origem, tais como incluir configurações adicionais em tvt.txt. Para instalar a partir da origem descompactada depois de fazer customizações, o usuário deve chamar msiexec.exe da linha de comandos, transmitindo o nome do arquivo msi descompactado. A seção a seguir descreve os parâmetros de linha de comandos disponíveis que podem ser utilizados com msiexec, bem como exemplos de como utilizá-los. As propriedades públicas também podem ser configuradas diretamente na chamada a msiexec na linha de comandos.

Parâmetros de Linha de Comandos de MsiExec.exe

MsiExec.exe é o programa executável do Windows Installer utilizado para interpretar os pacotes de instalação e instalar produtos em sistemas de destino.

```
msiexec. /i "C:WindowsFolder/Profiles\UserName\Persona\MySetups\nome do projeto
  \configuração do produto\nome do release\DiskImages\Disk1\nome do produto.msi
```

A tabela a seguir fornece uma descrição detalhada dos parâmetros de linha de comandos de MsiExec.exe. Essa tabela foi extraída diretamente da documentação do SDK da Plataforma Microsoft no Windows Installer.

Tabela 26.

Parâmetro	Descrição
/i *pacote* ou *código do produto*	Utilize este formato para formato o produto Othello: `msiexec /i "C:\WindowsFolder\Profiles\UserName\ Personal\MySetups\Othello\Trial Version\Release \DiskImages\Disk1\Othello Beta.msi"` Código do Produto refere-se ao GUID que é gerado automaticamente na propriedade de Código do Produto na visualização do projeto de seu produto.

Tabela 26. (continuação)

Parâmetro	Descrição
/f [p|o|e|d|c|a|u|m|s|v] *pacote* ou *código do produto*	A instalação com a opção /f reparará ou reinstalará arquivos ausentes ou corrompidos. Por exemplo, para forçar uma reinstalação de todos os arquivos, utilize a seguinte sintaxe: `msiexec /fa "C:\WindowsFolder\Profiles\UserName\ Personal\MySetups\Othello\Trial Version\Release \DiskImages\Disk1\Othello Beta.msi"` em conjunto com os seguintes sinalizadores: • p reinstala um arquivo se ele estiver ausente. • o reinstala um arquivo se ele estiver ausente ou se um versão mais antiga do arquivo estiver presente no sistema do usuário. • e reinstala um arquivo se ele estiver ausente ou se uma versão equivalente ou mais antiga do arquivo estiver presente no sistema do usuário. • c reinstala um arquivo se ele estiver ausente ou se o checksum armazenado do arquivo instalado não corresponder ao valor do novo arquivo. • a força uma reinstalação de todos os arquivos. • u ou m recria todas as entradas necessárias no registro do usuário. • s sobrescreve quaisquer atalhos existentes. • v executa o aplicativo a partir da origem e rearmazena em cache o pacote de instalação local.
/a *pacote*	A opção /a permite a usuários com privilégios de administrador instalar um produto na rede.
/x *pacote* ou *código do produto*	A opção /x desinstala um produto.
/L [i|w|e|a|r |u|c|m|p|v|+] *arquivo de log*	A construção com a opção /L especifica o caminho para o arquivo de registro—esses sinalizadores indicam quais informações devem ser gravadas no arquivo de registro: • i registra mensagens de status. • w registra mensagens de aviso não fatais. • e registra todas as mensagens de erro. • a registra o início de seqüências de ações. • r registra registros específicos da ação. • u registra pedidos do usuário. • c registra parâmetros iniciais da interface com o usuário. • m registra mensagens de falta de memória. • p registra configurações do terminal. • v registra a configuração de saída detalhada. • + anexa a um arquivo existente. • * é um caractere curinga que permite registrar todas as informações (excluindo a configuração de saída detalhada).

Tabela 26. (continuação)

Parâmetro	Descrição
/q [n|b|r|f]	A opção /q é utilizada para configurar o nível da interface com o usuário em conjunto com os seguintes sinalizadores: • q ou qn não cria uma interface com o usuário. • qb cria uma interface com o usuário básica. As configurações de interface com o usuário a seguir exibem uma caixa de diálogo modal no final da instalação: • qr exibe uma interface com o usuário reduzida. • qf exibe uma interface com o usuário completa. • qn+ não exibe uma interface com o usuário. • qb+ exibe uma interface com o usuário básica.
/? ou /h	Qualquer um dos comandos exibe informações de copyright do Windows Installer.
TRANSFORMS	Utilize o parâmetro de linha de comando TRANSFORMS para especificar quaisquer transformações que você gostaria de aplicar em seu pacote básico. A chamada da linha de comandos de transformação pode se assemelhar a esta: `msiexec /i "C:\WindowsFolder\Profiles\UserName\ Personal\MySetups\Nome do seu Projeto\Trial Version \My Release-1\DiskImages\Disk1\ProductName.msi" TRANSFORMS="New Transform 1.mst"` Você pode separar várias transformações com um ponto-e-vírgula. Portanto, recomenda-se não utilizar ponto-e-vírgula no nome da transformação, pois o serviço do Windows Installer os interpretará de maneira incorreta.
Propriedades	Todas as propriedades públicas podem ser definidas ou modificadas a partir da linha de comandos. As propriedades públicas se distinguem das propriedades privadas por estarem em letras maiúsculas. Por exemplo, COMPANYNAME é uma propriedade pública. Para configurar uma propriedade a partir da linha de comandos, utilize a seguinte sintaxe: PROPERTY=VALUE. Se você quisesse alterar o valor para COMPANYNAME, deveria digitar: `msiexec /i "C:\WindowsFolder\Profiles\UserName \Personal\MySetups\Your Nome do Projeto\Trial Version\My Release-1\DiskImages\Disk1\ProductName.msi" COMPANYNAME="InstallShield"`

Propriedades Públicas Padrão do Windows Installer

O Windows Installer tem um conjunto de propriedades públicas padrão incorporadas que podem ser configuradas na linha de comandos para especificar um determinado comportamento durante a instalação. As propriedades públicas mais comuns utilizadas na linha de comandos são descritas a seguir. Mais documentação está disponível no Web site da Microsoft em: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/about_properties.asp

A Tabela 3 mostra as propriedades do Windows Installer comumente utilizadas:

Tabela 27.

Propriedade	Descrição
TARGETDIR	Especifica o diretório de destino raiz para a instalação. Durante uma instalação administrativa esta propriedade é o local para copiar o pacote de instalação.
ARPAUTHORIZEDCDFPREFIX	URL do canal de atualização para o aplicativo.
ARPCOMMENTS	Fornece Comentários para Adicionar ou remover programas no Painel de controle.
ARPCONTACT	Fornece Contato para Adicionar ou remover programas no Painel de controle.
ARPINSTALLLOCATION	Caminho completo para a pasta primária do aplicativo.
ARPNOMODIFY	Desativa a funcionalidade que modificaria o produto.
ARPNOREMOVE	Desativa a funcionalidade que removeria o produto.
ARPNOREPAIR	Desativa o botão Reparar no assistente de Programas.
ARPPRODUCTICON	Especifica o ícone primário do pacote de instalação.
ARPREADME	Fornece um Leia-me para Adicionar ou remover programas no Painel de controle.
ARPSIZE	Tamanho estimado do aplicativo em kilobytes.
ARPSYSTEMCOMPONENT	Impede a exibição do aplicativo na lista Adicionar ou remover programas.
ARPURLINFOABOUT	URL para a home page de um aplicativo.
ARPURLUPDATEINFO	URL para informações de atualização do aplicativo.
REBOOT	A propriedade REBOOT suprime certos avisos para uma reinicialização do sistema Um administrador geralmente utiliza esta propriedade com uma série de instalações para instalar vários produtos ao mesmo tempo com somente uma reinicialização no final. Configure REBOOT=″R″ para desativar quaisquer reinicializações no final de uma instalação.
INSTALLDIR	Esta propriedade contém a pasta de destino padrão para os arquivos dos recursos e componentes.

Propriedades Pública Customizadas do Client Security Software

O pacote de instalação do programa Client Security Software contém um conjunto de propriedades públicas customizadas que podem ser configuradas na linha de comandos ao executar a instalação. As propriedades públicas customizadas

disponíveis são:

Tabela 28.

Propriedade	Descrição
EMULATIONMODE	Especifica que a instalação deve ser forçada no modo de Emulação mesmo se um TPM existir. Configure EMULATIONMODE=1 na linha de comandos para instalar no modo de Emulação.
HALTIFTPMDISABLED	Se o TPM estiver em um estado desativado e a instalação estiver executando no modo silencioso, o padrão é que a instalação prossiga no modo de emulação. Utilize a propriedade HALTIFTPMDISABLED=1 ao executar a instalação no modo silencioso para interromper a instalação se o TPM estiver desativado.
ENABLETPM	Configure ENABLETPM=0 na linha de comandos para impedir que a instalação ative o TPM.
NOPRVDISK	Configure NOPRVDISK=1 na linha de comandos para impedir que o recurso PrivateDisk do SafeGuard seja instalado. Isto é destinado a ser utilizado com uma instalação silenciosa mas pode ser utilizado também com uma instalação de UI. Na instalação de UI, o recurso PrivateDisk do SafeGuard não será mostrado na tela de configuração customizada.
NOPWMANAGER	Configure NOPWMANAGER=1 na linha de comandos para impedir que o recurso Password Manager seja instalado. Isto é destinado a ser utilizado com uma instalação silenciosa mas pode ser utilizado também com uma instalação de UI. Na instalação de UI, o recurso Password Manager não será mostrado na tela de configuração customizada.
NOCSSWIZARD	Configure NOCSSWIZARD=1 na linha de comandos para impedir que o Assistente CSS seja exibido quando um usuário administrativo efetuar logon e não tiver sido inscrito. Esta propriedade é destinada a alguém que deseje instalar o CSS mas utilizar scripts posteriormente para realmente configurar o sistema.
CSS_CONFIG_SCRIPT	Configure CSS_CONFIG_SCRIPT="*nome_do_arquivo*" ou "*nome_do_arquivo senha*" para fazer com que um arquivo de configuração seja executado depois que o usuário concluir a instalação e reinicializar.

Tabela 28. (continuação)

Propriedade	Descrição
SUPERVISORPW	Configure SUPERVISORPW=”*senha*” na linha de comandos para fornecer a senha do supervisor para ativar o chip no modo de instalação silencioso ou não silencioso. Se o chip estiver desativado e a instalação estiver executando no modo silencioso, a senha correta do supervisor deve ser fornecida para ativar o chip, caso contrário o chip não será ativado.

Arquivo de Registro da Instalação

Um arquivo de registro cssinstall60.log será criado no diretório %temp% se a instalação for ativada por setup.exe (dando um clique duplo no exe principal de instalação, executando o exe principal sem parâmetros ou extraindo o msi e executando setup.exe). Esse arquivo contém mensagens de registro que podem ser utilizadas para depurar problemas de instalação. Esse arquivo de registro não será criado ao executar o setup diretamente do pacote msi; isso inclui quaisquer ações executadas a partir de Adicionar ou remover programas. Para criar um arquivo de registro para todas as ações de MSI, você pode ativar a política de registro em log no registro. Para isso, crie o valor:

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

Exemplos de Instalação

A tabela a seguir mostra exemplos utilizando setup.exe:

Tabela 29.

Descrição	Exemplo
Instalação Silenciosa sem Reinicialização	`setup.exe /s /v"/qn REBOOT="R""`
Instalação Administrativa	`setup.exe /a`
Instalação Administrativa Silenciosa especificando o local de extração	`setup.exe /a /s /v"/qn TARGETDIR="F:\CSS60""`
Desinstalação Silenciosa setup.exe /s /x /v/qn	`setup.exe /s /x /v/qn`
Instalação sem Reinicialização e criação de um registro de instalação no diretório temp	`setup.exe /v"REBOOT="R" /L*v %temp%\cssinstall60.log"`
Instalação sem instalar o pré-desktop setup.exe /vPDA=0	`setup.exe /vPDA=0`

A tabela a seguir mostra exemplos de instalação utilizando o Solution.msi do Client Security:

Tabela 30.

Descrição	Exemplo
Instalar	`msiexec /i "C:\CSS60\Client Security Solution.msi"`
Instalação Silenciosa sem Reinicialização	`msiexec /i "C:\CSS60\Client Security Solution.msi" /qn REBOOT="R"`

Tabela 30. (continuação)

Descrição	Exemplo
Desinstalação Silenciosa	`msiexec /x "C:\CSS60\Client Security Solution.msi" /qn`

Instalação do System Migration Assistant

O procedimento de instalação do System Migration Assistant está documentado no *System Migration Assistant User's Guide*.

Instalação do Fingerprint Software

O arquivo setupo.exe do Fingerprint Software pode ser iniciado com os seguintes parâmetros:

Instalação Silenciosa

A instalação silenciosa do Fingerprint Software também é possível. Execute Setup.exe no diretório Install na unidade de CD-ROM.

Utilize a seguinte sintaxe:

```
Setup.exe PROPRIEDADE=VALOR /q /i
```

em que *q* é para instalação silenciosa e *i* é para instalar. Por exemplo:

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

Para desinstalar o software, utilize em vez disso o parâmetro /x:

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

Instalação por SMS

Instalações pelo SMS também são suportadas. Abra o Console do Administrador do SMS, crie um novo pacote e configure as propriedades do pacote de uma maneira padrão. Abra o pacote e selecione Novo-Programa no item Programas. Na linha de comandos, digite:

```
Setup.exe /m nome_de_seu_arquivo_mif /q /i
```

Você pode utilizar os mesmos parâmetros usados para a instalação silenciosa.

O setup normalmente reinicializa no final do processo de instalação. Se você quiser suprimir todas as reinicializações durante a instalação e reinicializar posteriormente (depois de instalar mais programas), inclua REBOOT="ReallySuppress" na lista de propriedades.

Opções

As seguintes opções são suportadas pelo Fingerprint Software:

Tabela 31.

Parâmetro	Descrição
CTRLONCE	Usado para exibir o Centro de Controle somente uma vez. O padrão é 0.
CTLCNTR	Usado para executar o Centro de Controle na inicialização. O padrão é 1.

Tabela 31. (continuação)

Parâmetro	Descrição
DEFFUS	#0 instalar nosso logon, não se importar com as configurações do FUS. (padrão para primeiras instalações, em Reparar/Modificar/Upgrade configurado como 1 se FUS estiver ativo) #1 detectar configurações do FUS no computador e tentar mantê-las.
INSTALLDIR	O diretório de instalação, padrão é fingerprint software.
OEM	• 0 = instalar o suporte para passaportes do servidor/autenticação do servidor. • 1 = Somente modo de computador independente com passaportes locais.
PASSPORT	O tipo de passaporte padrão configurado durante a instalação. • 1 = Padrão - passaporte local. • 2 = Passaporte do servidor. O padrão é 1.
SECURITY	• 1 - = Instalar o suporte para o modo protegido. • 0 = Não instalar; somente o modo conveniente existe.
SHORTCUTFOLDER	Nome padrão para pasta de atalho no menu Iniciar.
REBOOT	Pode ser usado para suprimir todas as reinicializações incluindo avisos durante a instalação, configurando como ReallySuppress.

Cenários de Software Instalado

Tabela 32.

Software Instalado	Notas
Client Security Software Versão 5.4x	Esta é a única versão do CSS suportada para coexistência com o Rescue and Recovery.
Rescue and Recovery Versão 3.0 somente	• Instalar por meio da instalação completa do produto, com o CSS não selecionado. • Alguns componentes do núcleo do Client Security Solution são instalados na instalação somente do RnR para suportar a criptografia de backups com o TPM, e para configuração da Senha Master de PDA.

Tabela 32. (continuação)

Software Instalado	Notas
Client Security Solution Versão 6.0 Independente.	• Este é um pacote de instalação separado. • Não é possível instalar o produto completo e cancelar a seleção do Rescue and Recovery para obter somente o Client Security Solution. • Os componentes do CSS (Private Disk e Password Manager) são opcionais.
Rescue and Recovery Versão 3.0 e Client Security Solution Versão 6.0	• Padrão de pré-carregamento - Instalar por meio da instalação normal do produto. • Componentes do CSS. • Private Disk e Password Manager são componentes opcionais.

Modificação do Estado do Software

Tabela 33.

Se o software instalado for o....	E você desejar mudar para o.....	Siga este processo.....	Notas	Construir
Client Security Software Versão 5.4x	Client Security Software 5.4x e Rescue and Recovery Versão 3.0	• Instale o produto. • Somente o componente Rescue and Recovery será instalado (nenhuma tela de configuração customizada é exibida). • Quando consultado, indique que você deseja manter o Client Security Software instalado.	• Os ganchos do Client Security Software para o Rescue and Recovery são implementados usando o modo de emulação. • Somente a Senha Master através do Client Security Software está disponível neste modo.	011
Client Security Software	Client Security Solution 6.0	• Desinstale o Client Security Software 5.4x • Instale o Client Security Solution 6.0 Independente.	Não é permitido tentar instalar o Client Security Solution Versão 6.0 sobre o Client Security Software Versão 5.4x. O usuário será avisado para remover primeiro o Client Security Software antigo.	011
Client Security Software	Rescue and Recovery Versão 3.0 e Client Security Solution Versão 6.0	• Desinstale o Client Security Software 5.4x • Instale o produto.	Uma tentativa de instalar o produto sobre o Client Security Software Versão 5.4x causará um aviso para remover primeiro o Client Security Software Versão 5.4x. Se a instalação prosseguir sem essa desinstalação, somente o Rescue and Recovery será instalado.	011

Tabela 34.

Se o software instalado for o....	**E você desejar mudar para o.....**	**Siga este processo.....**	**Notas**	**Construir**
Rescue and Recovery Versão 3.0	Client Security Software 5.4x e Rescue and Recovery Versão 3.0	• Desinstale o Rescue and Recovery • Instale o Client Security Software Versão 5.4x • Instale o produto conforme descrito acima	• Não é possível instalar o Client Security Software Versão 5.4x sobre nenhuma instalação do produto. • Os backups locais serão excluídos durante a desinstalação do Rescue and Recovery Versão 3.0.	011
Rescue and Recovery Versão 3.0	Client Security Solution 6.0	• Desinstale o Rescue and Recovery Versão 3.0 • Instale o Client Security Solution Versão 6.0 Independente.	• A desinstalação do Rescue and Recovery Versão 3.0 excluirá os arquivos do usuário e as configurações do registro do CSS. • Os backups do Rescue and Recovery Versão 3.0 protegidos com CSS não serão mais acessíveis. • Os backups locais serão excluídos durante a desinstalação do Rescue and Recovery Versão 3.0. • A instalação independente do Client Security Software Versão 6.0 não é permitida sobre nenhuma instalação do produto. • A opção 'Modificar' em Adicionar ou remover programas somente permitirá a adição do Client Security Solution neste caso. Não é possível remover o Rescue and Recovery através da opção 'Modificar'.	012
Rescue and Recovery Versão 3.0	Rescue and Recovery Versão 3.0 e Client Security Solution Versão 6.0	• Selecione a opção 'Modificar' em Adicionar ou remover programas. • Inclua o CSS e quaisquer componentes adicionais.	• Os backups locais serão excluídos quando o CSS for incluído. • O usuário será avisado ao incluir o Client Security Solution que deverá fazer novos backups depois de incluir o Client Security Solution. • As configurações e os arquivos de dados do Client Security Solution serão excluídos quando o Client Security Solution for incluído. • A instalação independente do Client Security Solution Versão 6.0 não é permitida sobre qualquer instalação do produto.	TBD

Tabela 35.

Se o software instalado for o....	**E você desejar mudar para o.....**	**Siga este processo.....**	**Notas**	**Construir**
Client Security Solution Versão 6.0 Independente.	Client Security Software 5.4x.	• Desinstale o Client Security Solution Versão 6.0 • Instale o Client Security Software Versão 5.4x.	• Não é possível instalar o Client Security Solution Versão 5.4x sobre nenhuma instalação do produto. • A desinstalação do Client Security Solution Versão 6.0 avisará sobre a exclusão de arquivos de dados e configurações. A opção selecionada aqui não causará impacto sobre a operação do Client Security Software Versão 5.4x.	011
Client Security Solution Versão 6.0 Independente.	Rescue and Recovery Versão 3.0.	• Desinstale o Client Security Solution Versão 6.0. • Instale o produto e escolha somente o Rescue and Recovery.	• A desinstalação do Client Security Solution Versão 6.0 avisará sobre a exclusão de arquivos do usuário e configurações da Versão do Client Security Solution. • A instalação do Rescue and Recovery 3.0 avisará ao usuário para remover quaisquer arquivos do usuário e configurações existentes do Client Security Solution. Se o usuário não optar por remover os arquivos, a instalação será cancelada.	012

Tabela 35. (continuação)

Se o software instalado for o....	E você desejar mudar para o.....	Siga este processo.....	Notas	Construir
Client Security Solution Versão 6.0 Independente.	Rescue and Recovery Versão 3.0 e Client Security Solution Versão 6.0.	• Execute a instalação do produto • As opções do Rescue and Recovery e Client Security Solution não podem ser desmarcadas. • Os componentes do Client Security Solution instalados anteriormente (Password Manager e Private Disk) são selecionados por padrão, mas essa seleção pode ser cancelada. Os componentes não instalados anteriormente estarão desmarcados por padrão, mas poderão ser selecionados.	• O Client Security Solution Versão 6.0 Independente será desinstalado sem aviso. • Os arquivos de dados e as configurações do Client Security Solution Versão 6.0 serão preservados. • O estado de emulação/não-emulação será preservado. • Após a conclusão da instalação do produto, o Assistente do Client Security Solution não será executado porque o Client Security Solution foi configurado anteriormente. • A opção para proteger os backups do Rescue and Recovery com o Client Security Solution deve ser feita através da GUI do Rescue and Recovery. Haverá uma opção para executar a GUI do Rescue and Recovery após a reinicialização na última tela da instalação. • Após a instalação do produto, as opções em Adicionar ou remover programas incluirão 'Remover', 'Reparar' e 'Modificar'. • A versão instalada do Client Security Solution Versão 6.0 deve ser igual a ou menor que a versão do produto que está sendo instalado, caso contrário, o usuário obterá uma mensagem indicando que o programa não pode ser instalado.	012

Notas:

1. Se o usuário instalar o Rescue and Recovery 3.0 silenciosamente, os arquivos do usuário e as configurações do Client Security Solution serão excluídos automaticamente durante a instalação.
2. Neste cenário, a seleção ou não do Password Manager e do Private Disk durante a instalação do produto (Rescue and Recovery 3.0 e Client Security

Solution 6.0) determinará o estado final do componente após a instalação do produto. Por exemplo, se o Password Manager tiver sido instalado com o Client Security Solution 6.0 e o usuário cancelar sua seleção durante a instalação do produto, ele não estará mais instalado após a conclusão da instalação. Se a instalação do produto (Rescue and Recovery e Client Security Solution) for executada silenciosamente, o Password Manager e o Private Disk serão instalados a menos que as respectivas propriedades NOPRVDISK=1 ou NOPWMANAGER=1 sejam configuradas no comando de instalação.

Tabela 36.

Se o software instalado for o....	**E você desejar mudar para o.....**	**Siga este processo.....**	**Notas**	**Construir**
Rescue and Recovery Versão 3.0 e Client Security Solution Versão 6.0	Client Security Software 5.4x	• Desinstale o produto • Instale o Client Security Solution Versão 5.4x	• Não é possível instalar o Client Security Software Versão 5.4x sobre nenhuma instalação do produto. • A desinstalação do produto avisará sobre a exclusão de arquivos de dados e configurações. A opção selecionada aqui não causará impacto sobre a operação do Client Security Software Versão 5.4x.	011
Rescue and Recovery Versão 3.0 e Client Security Solution Versão 6.0	Rescue and Recovery Versão 3.0	• Selecione a opção 'Modificar' em Adicionar ou remover programas. • Remova o Client Security Solution.	• Os backups locais serão excluídos quando o Client Security Solution for incluído. • A desinstalação do Client Security Solution avisará sobre a perda do PrivateDisk e do Password Manager. • Os backups do Rescue and Recovery Versão 3.0 protegidos com o Client Security Solution não serão mais acessíveis. • As configurações e os arquivos de dados do Client Security Solution serão excluídos quando o Client Security Solution for removido a partir de 'Modificar'.	TBD Não no Build 12

Tabela 36. (continuação)

Se o software instalado for o....	E você desejar mudar para o.....	Siga este processo.....	Notas	Construir
Rescue and Recovery Versão 3.0 e Client Security Solution Versão 6.0	Client Security Solution Versão 6.0	• Desinstale o produto. • A desinstalação avisará sobre a exclusão dos arquivos e configurações do Client Security Solution. Eles poderão ser mantidos se o usuário desejar manter a configuração existente do Client Security Solution. • Instale o Client Security Solution Versão 6.0 independente.	• Desinstale o produto. • A desinstalação avisará sobre a exclusão dos arquivos e configurações do Client Security Solution. Eles poderão ser mantidos se o usuário desejar manter a configuração existente do Client Security Solution. • Instale o Client Security Solution Versão 6.0 independente.	012

Notas:

1. Durante uma desinstalação do Client Security Solution 6.0 a partir de Adicionar ou remover programas, ou de uma desinstalação da interface com o usuário a partir da origem original, o usuário será avisado sobre a exclusão das configurações e arquivos de dados do CSS. Se a desinstalação for executada silenciosamente a partir da linha de comandos, o padrão é excluir as configurações e os arquivos de dados do CSS, porém, essa ação pode ser substituída configurando a propriedade NOCSSCLEANUP=1 no comando de desinstalação.
2. Durante uma desinstalação do produto (Rescue and Recovery e Client Security Solution 6.0) a partir de Adicionar ou remover programas, ou uma desinstalação da interface com o usuário a partir da origem original, o usuário será avisado para excluir as configurações e os arquivos de dados do Client Security Solution. Se a desinstalação for executada silenciosamente a partir da linha de comandos, o padrão é excluir as configurações e os arquivos de dados do Client Security Solution, porém, essa ação pode ser substituída configurando a propriedade NOCSSCLEANUP=1 no comando de desinstalação.

Capítulo 7. Infra-estrutura do Antidote Delivery Manager

O Antidote Delivery Manager funciona distribuindo instruções de um administrador para cada sistema e suportando comandos para combater um vírus ou um worm. O administrador prepara um script contendo as ações desejadas em cada sistema. A função repositório transmite o script com segurança ao sistema em minutos e executa os comandos. Os comandos incluem restrição a conexões de rede, exibição de mensagens aos usuários finais, restauração de arquivos a partir de backups, download de arquivos, execução de outros comandos do sistema e reinicialização da máquina no mesmo sistema operacional ou alternando dentro ou fora do ambiente do Rescue and Recovery. Tanto a função do repositório e os comandos funcionam no sistema operacional normal (como o Windows XP) ou no ambiente do Rescue and Recovery.

A estratégia global para combater um vírus é reduzir a propagação e os danos do código malicioso, aplicar correções e limpar cada sistema e, em seguida, devolver as máquinas restauradas novamente à rede. Para um vírus altamente destrutivo e de rápida propagação, poderá ser necessária a remoção de sistemas da rede e a condução de todas as operações de reparo no ambiente do Rescue and Recovery. Embora este seja o método mais seguro, ele produzirá também uma ruptura aos usuários finais se aplicado durante o expediente normal de trabalho. Em algumas circunstâncias, alternar para o ambiente do Rescue and Recovery poderá ser adiado ou evitado, restringindo-se os recursos da rede. A próxima etapa é transferir por download correções e o código de limpeza, e executar o código de limpeza e configurar as correções na instalação. Em geral, as correções devem ser instaladas durante a execução do sistema operacional, mas a limpeza e outras operações podem ser mais apropriadas no ambiente do Rescue and Recovery. Quando as ações corretivas forem concluídas, o sistema poderá então ser restaurado para a operação normal com o Windows XP em execução e as configurações de rede restauradas.

As duas seções a seguir descrevem a operação e os comandos do repositório em detalhes. Em seguida, são apresentadas a instalação e a configuração da função. As seções a seguir são exemplos de como utilizar o sistema para as tarefas comuns de teste, respondendo a vírus destrutivos, indicando máquinas conectadas por wireless ou VPNs (Redes Virtuais Privadas) e corrigindo problemas menos destrutivos.

Repositório

A função do repositório é executada em cada sistema e verifica periodicamente novas mensagens do administrador. Verifica em um intervalo de tempo planejado ou na ocorrência de vários eventos interessantes (por exemplo, inicialização, retomada de suspensão ou hibernação, detecção de um novo adaptador de rede e designação de um novo endereço IP). A função do repositório procura por mensagens em um conjunto de diretórios, em um local compartilhado do Windows, como \\machine\share\directory, em URLs de HTTP e em URLs de FTP. Se mais de uma mensagem for encontrada, ele as processa no “diretório classificado por nome”. Apenas uma mensagem é processada por vez. Uma mensagem só é processada com êxito uma vez. Se o processamento da mensagem falhar, por padrão, ela não será tentada novamente, mas tentar novamente ao falhar poderá ser especificado na própria mensagem.

Uma mensagem deve ser compactada por um administrador antes de ser colocada em um diretório para ser processada pela função do repositório. Para criar o pacote, o administrador coloca todos os arquivos que compõem a mensagem em um diretório (ou seus subdiretórios). Um dos arquivos deve ser denominado "GO.RRS", o script de comando principal. O administrador pode, opcionalmente, utilizar uma chave de assinatura para essa mensagem, mas se utilizada, a chave deverá estar disponível para todos os sistemas de destino. A função do repositório verifica a integridade do pacote, verifica se a assinatura foi fornecida e descompacta todos os arquivos em um diretório local antes de executar o GO.RRS.

O arquivo de script de comando principal (GO.RRS) segue a sintaxe de um arquivo de comando do Windows. Ele pode conter comandos legítimos do Windows e quaisquer dos comandos listados na próxima seção. Além disso, um interpretador de comandos Python é instalado como parte do ambiente do Rescue and Recovery, de modo que os scripts Python também podem ser chamados a partir do script GO.RRS.

No final da execução do script, todos os arquivos descompactados da mensagem são excluídos, portanto se os arquivos forem necessários após a saída do script (por exemplo, para instalar uma correção ao reinicializar), deverão ser retirados do diretório da mensagem.

Cada sistema possui uma configuração de repositórios a ser verificada. Poderá ser apropriado para o administrador de TI dividir a população de sistemas em grupos e designar repositórios diferentes (compartilhamentos de rede) a cada grupo. Por exemplo, os sistemas podem ser agrupados geograficamente por proximidade a um servidor de arquivos. Ou os sistemas podem ser agrupados por função, como engenharia, vendas ou suporte.

Comandos do Antidote Delivery Manager e Comandos Disponíveis do Windows

O sistema Antidote Delivery Manager fornece vários comandos para facilitar a operação do sistema. Além de o comando criar mensagens e ajustar as configurações, existem comandos para controlar a rede, determinar e controlar o estado do sistema operacional, examinar arquivos XML a partir de inventários do sistema e notificar o usuário final a respeito do progresso do script do Antidote Delivery Manager na máquina cliente. O comando NETWK ativa ou desativa a rede ou restringe a rede a um grupo limitado de endereços de rede. O comando INRR pode ser utilizado para determinar se o sistema operacional Windows XP está em execução ou se o computador está no ambiente do Rescue and Recovery. O comando REBOOT pode ser utilizado para encerrar o computador e especificar se ele deve inicializar no Windows XP ou no Rescue and Recovery. O aplicativo MSGBOX permite a comunicação com o usuário final exibindo uma mensagem em uma caixa pop-up. A caixa de mensagens pode, opcionalmente, conter os botões OK e Cancelar para que a mensagem possa agir de modo diferente, dependendo da entrada do usuário final.

Determinados comandos Microsoft também estão disponíveis no Antidote Delivery Manager. Os comandos permitidos incluem todos os comandos criados no shell de comandos, por exemplo, DIR ou CD. Outros comandos úteis, como REG.EXE para alterar o registro e CHKDSK.EXE para verificar a integridade do disco, estão disponíveis.

Utilização Típica do Antidote Delivery Manager

O sistema Antidote Delivery Manager pode ser utilizado para concluir uma variedade de tarefas. Os exemplos a seguir demonstram como o sistema pode ser utilizado.

- **Teste de Sistema Simples - Exibir notificação**

  O uso mais básico do sistema é para exibir uma simples mensagem ao usuário final. A maneira mais fácil de executar esse teste e também de testar outros scripts antes da implementação é colocar a mensagem em um repositório que esteja em um diretório local no computador pessoal do administrador. Essa colocação permite o teste rápido do script sem impacto em outras máquinas.

- **Preparo e Compactação do Script**

  Gravar um script GO.RRS em qualquer máquina em que o Antidote Delivery Manager esteja instalado. Inclua uma linha: `MSGBOX /MSG "Hello World" /OK`. Execute o comando APKGMSG no diretório contendo o GO.RRS para criar uma mensagem.

- **Execução do Script**

  Coloque o arquivo de mensagens em um dos diretórios do repositório em sua máquina e observe se a operação está correta. Na próxima vez em que o agente de correio for executado, uma caixa de mensagens será exibida com o texto "Hello World". Esse script é também uma boa maneira de testar repositórios de rede e demonstrar recursos, como a verificação de repositórios na retomada do modo de suspensão.

Principais Ataques de Worms

O exemplo demonstra uma possível abordagem para combater um vírus principal. A abordagem básica é desligar a rede e, em seguida, reinicializar o Rescue and Recovery, recuperar as correções, executar os reparos e então inicializar novamente o Windows XP, instalar as correções e, finalmente, restaurar a rede. Uma única mensagem pode ser utilizada para executar todas essas funções por meio do uso de arquivos sinalizadores e do comando RETRYONERROR.

1. **Fase de Travamento**

   A primeira coisa a fazer é informar o usuário final sobre o que aconteceu. Se o ataque não for extremamente sério, o administrador poderá dar ao usuário final a opção de adiar a correção para depois. No caso mais conservador, essa fase deveria ser utilizada para desativar a rede e fornecer uma janela de atalho, como, por exemplo, 15 minutes para que o usuário final salve o trabalho em progresso. RETRYONERROR é utilizado para manter o script em execução e, em seguida, a máquina poderá ser reinicializada no ambiente do Rescue and Recovery.

2. **Fase de Distribuição do Código - uma fase de reparo**

   Agora que o perigo de infecção foi removido pela desativação da rede e pela reinicialização do Rescue and Recovery, o código adicional poderá ser recuperado e os reparos executados. A rede poderá ser ativada ou apenas alguns endereços serão permitidos no momento necessário para recuperar arquivos adicionais. Enquanto estiver no Rescue and Recovery, os arquivos de vírus poderão ser removidos e o registro poderá ser limpo. Infelizmente, a instalação de um novo software ou de correções não será possível, pois as correções supõem que o Windows XP esteja em execução. Com a rede ainda desativada e todos os códigos de vírus removidos, é seguro reinicializar o Windows XP para concluir os reparos. Um arquivo de tags gravado neste momento direciona o script para a seção de correção após a reinicialização.

3. **Fase de Correção e Recuperação**

Quando a máquina reinicializa no Windows XP, o Antidote Delivery Manager começa a processar novamente, mesmo antes de o usuário final efetuar login. As correções devem ser instaladas nesse momento. A máquina poderá ser reinicializada no final se as correções recém-instaladas exigirem isso. Agora que toda a limpeza e as correções foram concluídas, a rede poderá ser ativada e o usuário final informado de que a operação normal é possível.

Atualização Secundária de Aplicativo

Nem toda manutenção requer as medidas drásticas descritas anteriormente. Se uma correção estiver disponível, mas um ataque por vírus não estiver em progresso, uma abordagem mais branda poderia ser mais apropriada.

Um único script pode controlar a operação por meio do uso do RETRYONERROR e dos arquivos de tags.

1. **Fase de Download**

   O processo começa com uma caixa de mensagens informando o usuário final de que uma correção será transferida por download para posterior instalação. Em seguida, a correção poderá ser copiada do servidor.

2. **Fase de Correção**

   Agora que o código da correção já está pronto para instalação, é o momento de avisar o usuário final e iniciar a instalação. Se o usuário final solicitar um retardo, um arquivo de tags poderia ser utilizado para rastrear o retardo. Talvez as solicitações posteriores para instalação da correção sejam mais urgentes. Observe que o Antidote Delivery Manager mantém este estado mesmo se o usuário final desligar ou reinicializar o sistema. Quando o usuário final tiver permissão concedida, a correção será instalada e o sistema será reinicializado, se for necessário.

Acomodando VPNs e Segurança de Wireless

O ambiente do Rescue and Recovery não suporta atualmente VPNs (Redes Virtuais Privadas) de acesso remoto nem conexão de rede wireless. Se uma máquina estiver utilizando uma dessas conexões de rede no Windows XP e, em seguida, reinicializar o Rescue and Recovery, a conectividade da rede será perdida. Entretanto, um script como o do exemplo anterior não funcionará, pois a rede não está disponível no Rescue and Recovery para fazer download de arquivos e correções.

A solução é compactar todos os arquivos necessários na mensagem original ou fazer download dos arquivos necessários antes de reinicializar. Isso é feito colocando todos os arquivos necessários no diretório com GO.RRS. O arquivo de script deve ser cauteloso ao mover os arquivos necessários para suas posições finais antes de sair do script (quando o diretório que contém o GO.RRS no cliente for excluído). A colocação de correções no arquivo de mensagens poderá não ser prática se as correções forem muito grandes. Nesse caso, o usuário final deverá ser informado e a rede restringida apenas ao servidor que contém a correção. Em seguida, a correção poderá ser transferida por download ainda estando no Windows XP. Embora isso possa prolongar a exposição do Windows XP a um vírus, o tempo extra provavelmente não será significativo.

Capítulo 8. Boas Práticas

Este capítulo apresenta cenários de uso para ilustrar as boas práticas do Rescue and Recovery, Client Security Solution e ThinkVantage Fingerprint Software. Este cenário começa com a configuração da unidade de disco rígido, continua com as várias atualizações e segue o ciclo de vida de uma implementação. A instalação em computadores IBM e não-IBM é descrita.

Exemplos de Implementação para Instalação do Rescue and Recovery e do Client Security Solution

A seguir, alguns exemplos da instalação do Rescue and Recovery e do Client Security Solution em uma máquina ThinkCentre e um ThinkPad.

Exemplo de Implementação no ThinkCentre

Este é um exemplo de instalação em um ThinkCentre, utilizando estes requisitos hipotéticos do cliente:

- **Administração**
  - Criar Backup Básico do Sysprep com o Rescue and Recovery.
  - Utilizar a conta Administrador local para administração do computador.
- **Rescue and Recovery**
  - Utilizar a passphrase do Client Security para proteger o acesso ao espaço de trabalho do Rescue and Recovery.
    - O usuário deve efetuar login com sua passphrase e poderá abrir o arquivo do volume SafeGuard PrivateDisk para resgatar arquivos.
- **Client Security Solution**
  - Instalar e executar no Modo de Emulação.
    - Nem todos os sistemas IBM possuem um Módulo Confiável da Plataforma (chip de segurança).
  - Sem Gerenciador de Senhas.
    - Em vez disso, o cliente está utilizando uma solução de conexão simples corporativa.
  - Ativar a passphrase do Client Security.
    - Proteger os aplicativos do Client Security Solution por meio de uma passphrase.
  - Ativar o logon do Windows do Client Security.
    - Efetuar login no Windows com a passphrase do Client Security.
  - Criar SafeGuard PrivateDisk para todos os usuários com um tamanho de 500 MB.
    - Cada usuário precisa de 500 MB de espaço para armazenar dados com segurança.
  - Ativar o recurso de Recuperação de Passphrase do Usuário Final.
    - Permitir que os usuários recuperem sua passphrase respondendo às três perguntas e respostas definidas pelo usuário.
  - Criptografar o Script XML do Client Security Solution com a senha = "XMLscriptPW".
    - A senha protege o arquivo de configuração do Client Security Solution.

Na máquina de preparação:

1. Efetue login na conta "Administrador Local" do Windows.
2. Instale o programa Rescue and Recovery e Client Security Solution com as seguintes opções:

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

   Notas:

   a. Assegure-se de que o arquivo ou arquivos tvt, como z062zaa1025us00.tvt, estejam localizados no mesmo diretório do arquivo executável ou a instalação falhará.

   b. Se o nome do arquivo for setup_tvtrnr3_1027c.exe, então você fez download do pacote combinado. Essas instruções são para os arquivos que podem ser transferidos separadamente por download a partir da página de download de arquivos de idioma individual de uma Grande Empresa.

   c. Se você estiver executando uma instalação do administrador, consulte "Instalando o Rescue and Recovery em um Novo Lançamento de Computadores Lenovo e IBM" na página 118.

3. Depois de reinicializar, efetue login com a conta Administrador local do Windows e prepare o script XML para implementação. Na linha de comandos, execute este comando

   ```
   "C:\Program Files\IBM ThinkVantage\Client Security Solution\css_wizarde.exe"
   /name:C:\ThinkCentre
   ```

   Selecione as seguintes opções no Assistente:

   - Selecione **Avançado -> Avançar**
   - Selecione **Passphrase do Client Security -> Avançar**
   - Selecione **Efetuar Logon com a Tela de Login do Client Security -> Avançar**
   - Digite a senha do Windows da conta Administrador **-> Avançar**

     (WPW4Admin por exemplo)
   - Digite a passphrase do Client Security da conta Administrador, marque a caixa de diálogo **Utilizar a passphrase do Client Security para proteger o acesso ao espaço de trabalho do Rescue and Recovery -> Avançar**

     (CSPP4Admin por exemplo)
   - Marque a caixa de diálogo **Ativar Recuperação de Senha** e selecione três perguntas e respostas da conta Administrador **-> Avançar**

     a. Qual o nome do seu primeiro animal de estimação?

        (Felpudo, por exemplo)

     b. Qual o seu filme favorito?

        (E o Vento Levou, por exemplo)

     c. Qual o seu time favorito?

        (São Paulo, por exemplo)
   - Não marque **Criar um volume PrivateDisk para cada usuário, com o tamanho selecionado abaixo**. **-> Avançar**
   - Revise o Resumo e selecione **Aplicar** para gravar o arquivo xml no seguinte local C:\ThinkCentre.xml **-> Aplicar**
   - Selecione **Concluir** para fechar o assistente.

4. Abra o arquivo a seguir em um editor de texto (editores de script XML ou Microsoft Word 2003 possuem recursos de formato XML internos) e modifique as seguintes configurações:

- Remova todas as referências à configuração de Domínio. Isso informará ao script para utilizar o nome da máquina local em cada sistema. Salve o arquivo.

5. Utilize a ferramenta encontrada em C:\Program Files\IBM ThinkVantage\Client Security Solution\xml_crypt_tool.exe para criptografar o script XML com uma senha. Execute o arquivo a partir de um prompt de comandos, utilize a seguinte sintaxe:
   a. xml_crypt_tool.exe C:\ThinkCentre.xml /encrypt XMLScriptPW.
   b. Agora, o arquivo se chamará C:\ThinkCentre.xml.enc e estará protegido pela senha = XMLScriptPW.

Agora, o arquivo C:\ThinkCentre.xml.enc está pronto para ser incluído na máquina de implementação.

Na máquina de implementação:

1. Efetue login com a conta Administrador local do Windows.
2. Instale os programas Rescue and Recovery e Client Security Solution com as seguintes opções:

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

   Notas:
   a. Assegure-se de que o arquivo ou arquivos tvt, como z062zaa1025us00.tvt, estejam localizados no mesmo diretório do arquivo executável ou a instalação falhará.
   b. Se o nome do arquivo for setup_tvtrnr3_1027c.exe, então você fez download do pacote combinado. Essas instruções são para os arquivos que podem ser transferidos separadamente por download a partir da página de download de arquivos de idioma individual de uma Grande Empresa.
   c. Se você estiver executando uma instalação do administrador, consulte "Instalando o Rescue and Recovery em um Novo Lançamento de Computadores Lenovo e IBM" na página 118.
3. Depois de reinicializar, efetue login com a conta Administrador Local do Windows.
4. Inclua o arquivo ThinkCentre.xml.enc anteriormente preparado no diretório raiz C:\.
5. Modifique o Registro para definir o Tamanho do Volume SafeGuard PrivateDisk padrão = 500 MB para todos os usuários. Isso é facilmente executado importando um arquivo *reg*:
   a. Vá para: HKEY_LOCAL_MACHINE\SOFTWARE\IBM ThinkVantage\Client Security Software.
   b. Crie um novo Valor de Cadeia com o Nome de Valor: = PrivateDiskSize e uma Data de Valor: = 500.
   c. Crie um Valor DWORD com o Nome de Valor: = UsingPrivateDisk e uma Data de Valor: = 1.
6. Prepare o comando RunOnceEx com os seguintes parâmetros.
   - Inclua uma nova chave na chave RunonceEx, chamada "0001". Ela deve ser: HKEY_LOCAL_MACHINE \Software\Microsoft\Windows\Current Version\RunOnceEx\0001
   - Nessa chave, inclua um nome de valor de cadeia "CSSEnroll" com o valor: "c:\program files\IBM ThinkVantage\Client Security Solution\vmservere.exe" C:\ThinkCenter.xml.enc XMLscriptPW

7. Execute “%rr%\rrcmd.exe sysprepbackup location=L name=”Sysprep Backup”. Depois que o sistema estiver preparado, voce verá esta saída:

```
*****************************************************
** 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. Execute sua implementação do Sysprep agora.
9. Encerre e reinicialize sua máquina. Ela iniciará o processo de backup no Windows PE.

   Nota: NOTA: Ela dirá que a restauração está em progresso, mas um backup estará ocorrendo. Depois do backup, DESLIGUE A POWER, não reinicie.

Agora, o backup básico do Sysprep está completo

Exemplo de Implementação no Thinkpad

Este é um exemplo de instalação em um ThinkPad, utilizando estes requisitos hipotéticos do cliente:

- **Administração**
  - Instalar em sistemas já com imagens e implementados.
  - Utilizar a conta Administrador de domínio para administração do computador.
  - Todos os computadores têm uma senha de supervisor da BIOS, BIOSpw.
- **Client Security Solution**
  - Alavancar o Módulo Confiável da Plataforma.
    - Todos as máquinas têm o chip de segurança.
  - Ativar o Gerenciador de Senhas.
  - Desativar o SafeGuard PrivateDisk.
    - Em vez disso, alavancar a criptografia total da unidade de disco rígido do Utimaco SafeGuard Easy.
  - Alavancar senha de usuários do Windows, como autenticação do Client Security Solution.
    - Permite uma única senha do Windows para autenticação do Utimaco SafeGuard Easy, Client Security Solution e do Domínio do Windows.
  - Criptografar o Script XML do Client Security Solution com a senha = ″XMLscriptPW″.
    - A senha protege o arquivo de configuração do Client Security Solution.
- **ThinkVantage Fingerprint Software**
  - Não alavancar as senhas da BIOS e da unidade de disco rígido.
  - Efetuar logon com Impressão Digital.
    - Após um período inicial de inscrição automática do usuário, o usuário efetuará logon no Modo de Segurança requerendo uma Impressão Digital para usuários não-administradores, além de forçar efetivamente uma metodologia de autenticação de fator duplo.
  - Incluir o Tutorial de Impressão Digital.
    - Os usuários finais podem aprender a posicionar corretamente o dedo e obter um feedback visual do que pode estar fazendo de errado.

Na máquina de preparação:

1. A partir do estado desativado, inicie o computador e pressione **F1** para acessar a BIOS e navegar para o menu Segurança e limpar o Chip de Segurança. Salvar e Sair da BIOS.
2. Efetue login com a conta Administrador de Domínio do Windows.
3. Instale o ThinkVantage Fingerprint Software executando o f001zpz2001us00.exe para extrair o arquivo setup.exe do pacote da Web. Isso extrairá automaticamente o setup.exe no seguinte local: C:\IBMTOOLS\APPS\TFS4.6-Build1153\Application\0409\setup.exe.
4. Instale o ThinkVantage Fingerprint Tutorial executando o f001zpz7001us00.exe para extrair o arquivo tutess.exe do pacote da Web. Isso extrairá automaticamente o setup.exe no seguinte local: C:\IBMTOOLS\APPS\tutorial\TFS4.6-Build1153\Tutorial\0409\tutess.exe.
5. Instale o ThinkVantage Fingerprint Console executando o f001zpz5001us00.exe para extrair o arquivo fprconsole.exe do pacote da Web. Executar o f001zpz5001us00.exe extrairá o setup.exe no seguinte local: C:\IBMTOOLS\APPS\fpr_con\APPS\UPEK\FPR Console\TFS4.6-Build1153\Fprconsole\fprconsole.exe.
6. Instale o programa Client Security Solution com as seguintes opções:

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

7. Depois de reinicializar, efetue login com a conta Administrador de Domínio do Windows e prepare o script XML para implementação. Na linha de comandos, execute:

   ```
   "C:\Program Files\IBM ThinkVantage\Client Security Solution\css_wizard.exe"
   /name:C:\ThinkPad.
   ```

   Selecione as seguintes opções no Assistente para corresponder ao script de exemplo:

   - Selecione Avançado **-> Avançar**
   - Selecione Senha do Windows **-> Avançar**
   - Selecione Efetuar logon com o sensor de impressão digital **-> Avançar**
   - Digite a senha do Windows da conta Administrador de Domínio **-> Avançar** (WPW4Admin por exemplo)
   - Desmarque Ativar Recuperação de Senha **-> Avançar**
   - Revise o Resumo e selecione Aplicar para gravar o arquivo xml no seguinte local C:\ThinkPad.xml.
   - Selecione **Concluir** para fechar o assistente.
8. Utilize a ferramenta encontrada em C:\Program Files\IBM ThinkVantage\Client Security Solution\xml_crypt_tool.exe para criptografar o script XML com uma senha. Em um prompt de comandos, utilize a seguinte sintaxe:
   a. xml_crypt_tool.exe C:\ThinkPad.xml /encrypt XMLScriptPW.
   b. O arquivo se chamará C:\ThinkPad.xml.enc e estará protegido pela senha = XMLScriptPW.

Na máquina de implementação:

1. Utilizando as ferramentas de distribuição de software da empresa, implemente o executável setup.exe do ThinkVantage Fingerprint Software que foi extraído da máquina de preparação para cada máquina de implementação. Quando o setup.exe for enviado para a máquina, instale-o utilizando o seguinte comando:

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

2. Utilizando as ferramentas de distribuição de software da empresa, implemente o executável tutess.exe do ThinkVantage Fingerprint Tutorial que foi extraído da máquina de preparação para cada máquina de implementação. Quando o tutess.exe for enviado para a máquina, instale-o utilizando o seguinte comando:

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

3. Utilizando as ferramentas de distribuição de software da empresa, implemente o executável fprconsole.exe do ThinkVantage Fingerprint Console que foi extraído da máquina de preparação para cada máquina de implementação.
   - Coloque o arquivo fprconsole.exe no diretório "C:\Program Files\ThinkVantage Fingerprint Software\".
   - Desligue o suporte de segurança da BIOS Power-on, executando o seguinte comando: fprconsole.exe settings TBX 0.
4. Utilizando as ferramentas de distribuição de software da empresa, implemente o executável "setup_tvtcss6_1027.exe" do ThinkVantage Client Solution.
   - Quando o setup_tvtcss6_1027.exe for enviado para a máquina, instale-o utilizando o seguinte comando: setup_tvtcss6_1027.exe /s /v"/qn NOPRVDISK=1 NOCSSWIZARD=1 SUPERVISORPW="BIOSpw"".
   - A instalação do software ativará automaticamente o hardware do Módulo Confiável da Plataforma.
5. Depois de reinicializar o sistema, configure-o por meio do arquivo de script XML, utilizando o seguinte procedimento:
   - Copie o arquivo ThinkPad.xml.enc preparado anteriormente no diretório C:\.
   - Execute o C:\Program Files\IBM ThinkVantage\Client Security Solution\vmserver.exe C:\ThinkPad.xml.enc XMLScriptPW.
6. Depois de uma reinicialização, o sistema estará pronto para a inscrição do usuário do Client Security Solution. Todos os usuários poderão efetuar login no sistema com o ID do Usuário e a senha do Windows. Todo usuário que efetuar login no sistema será solicitado automaticamente a se inscrever no Client Security Solution e, em seguida, inscrever-se no leitor de impressão digital.
7. Depois que todos os usuários do sistema estiverem inscritos no ThinkVantage Fingerprint Software, a configuração do Modo de Segurança poderá ser ativada para forçar que todos os usuários não-administradores do Windows efetuem logon com impressão digital.
   - Execute o seguinte comando: C:\Program Files\ThinkVantage Fingerprint Software\fprconsole.exe settings securemode 1.
   - Para remover a mensagem Pressione CTRL+ALT+DEL para efetuar logon utilizando uma senha. Na tela de logon, execute o seguinte comando:

     ```
     C:\Program Files\ThinkVantage Fingerprint Software\fprconsole.exe settings
     CAD 0
     ```

Agora, a implementação do Client Security Solution 6.0 e do ThinkVantage Fingerprint Software está completa.

Instalando o Rescue and Recovery em um Novo Lançamento de Computadores Lenovo e IBM

Esta seção descreve a instalação do Rescue and Recovery em um novo lançamento.

Preparando a Unidade de Disco Rígido

A primeira etapa a ser considerada ao implementar um sistema é preparar a unidade de disco rígido do sistema doador. Para assegurar-se de que esteja iniciando com um disco rígido vazio, você deve limpar o Registro de Inicialização Principal do disco rígido principal.

1. Remova todos os dispositivos de armazenamento, como discos rígidos secundários, discos rígidos USB, chaves de memória USB, Memória PC Card, etc., do sistema doador, exceto o disco rígido principal no qual você irá instalar o Windows.

   Atenção: A execução desse comando apagará todo o conteúdo da unidade de disco rígido de destino. Depois de executá-lo, não será possível recuperar quaisquer dados da unidade de disco rígido de destino.
2. Crie um disquete de inicialização em DOS e coloque nele o arquivo CLEANDRV.EXE.
3. Inicialize o disquete (apenas um dispositivo de armazenamento conectado). No prompt do DOS, digite o seguinte comando:

   ```
   CLEANDRV /HDD=0
   ```
4. Instale o sistema operacional e os aplicativos. Construa o seu sistema doador como se você não estivesse instalando o Rescue and Recovery. A última etapa do processo é instalar o Rescue and Recovery.

Instalação

Esta primeira etapa do processo de instalação é a extração do executável InstallShield no diretório C:\RRTEMP. Se você for instalar o Rescue and Recovery em vários sistemas, a execução desse processo uma vez reduzirá pela metade o tempo de instalação em cada máquina.

1. Supondo-se que o arquivo de instalação esteja localizado na raiz da unidade C, crie um arquivo EXE_EXTRACT.CMD, que extrairá o arquivo C:\SETUP_TVTRNR3_*XXXX*.EXE (em que *XXXX* é o ID de construção) no diretório C:\RRTEMP:

   ```
   :: This package will extract the WWW EXE to the directory c:\RRTemp for an
   :: administrative install.
   @ECHO OFF
   :: This is the name of the EXE (Without the .EXE)
   set BUILDID=setup_tvtrnr3_1027.exe
   :: This is the drive letter for the Setu_tvtrnr3_1027.exe
   :: NOTE: DO NOT END THE STRING WITH A "\".  IT IS ASSUMED TO NOT BE THERE.
   SET SOURCEDRIVE=C:
   :: Create the RRTemp directory on the HDD for the exploded WWW EXMD c:\RRTemp
   :: Explode the WWW EXE to the directory c:\RRTemp
   :: Note: The TVT.TXT file must be copied into the same directory as the
   :: MSI.EXE file.
   start /WAIT %SOURCEDRIVE%\%BUILDID%.exe /a /s /v"/qn TARGETDIR=c:\RRTemp"
    TARGETDIR=c:\RRTemp"
   Copy Z062ZAA1025US00.TVT C:\rrtemp\
   ```
2. Você pode fazer várias personalizações antes da instalação do Rescue and Recovery. Alguns exemplos deste cenário são:
   - Altere o número máximo de backups incrementais para 4.
   - Defina o Rescue and Recovery para executar um backup incremental diariamente às 13h59 no disco rígido local e chame-o de Planejado.
   - Oculte a interface com o usuário do Rescue and Recovery de todos os usuários que não façam parte do Grupo de Administradores.

3. Crie um arquivo TVT.TXT personalizado. Alguns parâmetros podem ser modificados. Consulte Apêndice B, “Configurações e Valores do TVT.TXT”, na página 141 para obter informações adicionais.

```
[Scheduler]
Task1=RescueRecovery
Task2=egathererTask3=logmon

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


[RescueRecovery]
LastBackupLocation=1
CustomPartitions=0
Exclude=0Include=0MaxNumberOfIncrementalBackups=5
EncryptUsingCSS=0
HideCSSEncrypt=0
UUIDMatchRequired=0
PasswordRequired=0DisableSchedule=0
DisableRestore=0
DisableSFR=0DisableViewBackups=0
DisableArchive=0DisableExclude=0
DisableSingleStorage=0
DisableMigrate=0
DisableDelete=0
DisableAnalyze=0
DisableSysprep=1
CPUPriority=3
Yield=0Ver=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=2ScheduleHour=12
ScheduleMinute=0ScheduleDayOfTheMonth=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. No mesmo diretório do arquivo TVT.TXT personalizado, crie um arquivo INSTALL.CMD, que executará várias ações:
   - Copie o arquivo TVT.TXT personalizado no pacote de instalação criado no diretório C:\RRTemp:
   - Execute uma instalação silenciosa do Rescue and Recovery sem uma reinicialização no final.
   - Inicie o Rescue and Recovery para que um backup básico possa ser feito.
   - Depois que o serviço for iniciado, configure o ambiente para criar uma imagem ISO do CD do Rescue and Recovery (isso é normalmente executado como parte de uma reinicialização).
   - Crie a imagem ISO.
   - Crie o backup básico e reinicialize o sistema.
5. Modifique o código INSTALL.CMD. O conteúdo a seguir representa o código INSTALL.CMD:

```
:: Copy custom TVT.txt here

copy tvt.txt "c:\RRTemp\Program Files\IBM ThinkVantage\Rescue and Recovery"

:: Install using the MSI with no reboot (Remove "REBOOT="R"" to force a reboot)

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

:: Start the service. This is needed to create a base backup.

start /WAIT net start "Rescue and Recovery Service"

:: Make an ISO file here - ISO will reside in c:\Program Files\IBM
ThinkVantage\Rescue and Recoveery\rrcd
```

Nota: Você não precisa configurar o ambiente se o sistema for reinicializado.

```
:: Set up the environment

set PATH=%PATH%;%SystemDrive%\Program Files\IBM ThinkVantage\Common\Python24

set PATHEXT=%PATHEXT%;.PYW;.PYO;.PYC;.PY

set TCL_LIBRARY=%SystemDrive%\Program Files\IBM ThinkVantage\Common\Python24
\tcl\tcl8.4

set TK_LIBRARY=%SystemDrive%\Program Files\IBM ThinkVantage\Common\Python24
\tcl\tk8.4

set PYTHONCASEOK=1

set RR=C:\Program Files\IBM ThinkVantage\Rescue and Recovery\

set PYTHONPATH=C:\Program Files\IBM ThinkVantage\Common\logger

:: The next line will create the ISO silently and not burn it

C:\Program Files\IBM ThinkVantage\Common\Python24\python C:\Program Files\IBM
ThinkVantage\Common\spi\mkspiim.pyc /scripted

:: Take the base backup... service must be started

c:

cd "C:\Program Files\IBM ThinkVantage\Rescue and Recovery"
```

```
RRcmd.exe backup location=L name=Base level=0
:: Reboot the system
C:\Program Files\IBM ThinkVantage\Common\BMGR\bmgr32.exe /R
```

Personalização

Você implementou o Rescue and Recovery em seu ambiente e deseja alterar os seguintes itens com o Rescue and Recovery:

- Você deseja fazer mais do que 4 backups incrementais e gostaria de alterá-lo para 10.
- O horário de backup às 13h59 interfere de alguma maneira em seu ambiente. Você gostaria de alterá-lo para às 10h24.
- Você deseja permitir que todos os sistemas acessem a interface com o usuário Rescue and Recovery 3.0.
- Você deseja divulgar o sistema para outros processos durante um backup planejado. Sua avaliação após a experimentação determina que o valor correto de `Yield=` em seu ambiente deveria ser `2` em vez do valor padrão de `0`.

Para fazer essas alterações em várias máquinas:

1. Crie um arquivo mod denominado UPDATE.MOD (utilizando um editor de texto) com o seguinte conteúdo:

   ```
   [RescueRecovery] MaxNumberOfIncrementalBackups=10
   [rescuerecovery] ScheduleHour=10
   [rescuerecovery] ScheduleMinute=24
   [rescuerecovery] GUIGroup=
   [rescuerecovery] Yield=2
   ```

2. Você pode então criar um arquivo INSTALL.CMD e utilizar uma ferramenta de gerenciamento de sistema de sua preferência para enviar os arquivos INSTALL.CMD e UPDATE.MOD para os seus sistemas de destino. Depois que os sistemas executarem o arquivo INSTALL.CMD, as atualizações se tornarão efetivas. O conteúdo do arquivo INSTALL.CMD é o seguinte:

   ```
   :: Merge the changes into TVT.TXT
   "%RR%cfgmod.exe" "%RR%tvt.txt" update.mod
   :: Reset the scheduler to adopt the new scheduled backup time without a reboot
   "%RR%reloadsched.exe"
   ```

Atualizando

Talvez seja necessário fazer uma grande alteração em seu sistema, como uma atualização no Service Pack do Windows. Antes de instalar o Service Pack, force um backup incremental no sistema e identifique esse backup por nome, executando as seguintes etapas:

1. Crie um arquivo FORCE_BU.CMD e envie-o para os sistemas de destino.
2. Ative o arquivo FORCE_BU.CMD se ele estiver no sistema de destino.

O conteúdo do arquivo FORCE_BU.CMD é:

```
:: Force a backup now
"%RR%rrcmd" backup location=L name="Backup Before XP-SP2 Update"
```

Ativando o Desktop do Rescue and Recovery

Depois de compreender os benefícios do Rescue and Recovery por algum tempo, talvez você queira se beneficiar do ambiente do Rescue and Recovery. Para fins de demonstração, um script de amostra UPDATE_RRE.CMD será fornecido na próxima seção que extrairá o arquivo de controle no ambiente do Rescue and Recovery, o qual você poderá editar e, em seguida, devolver ao ambiente do

Rescue and Recovery utilizando RRUTIL.exe. Consulte “Utilizando o RRUTIL.EXE” na página 20 para obter informações adicionais.

Para modificar a Área Pré-desktop, o script UPDATE_RRE.CMD demonstra vários processos:

- Utilize o RRUTIL.exe para obter um arquivo do ambiente do Rescue and Recovery. Os arquivos a serem extraídos do ambiente do Rescue and Recovery são definidos no arquivo GETLIST.TXT.
- Crie uma estrutura de diretórios para devolver os arquivos à Área Pré-desktop, depois de editar o arquivo apropriado.
- Faça uma cópia do arquivo por segurança e, em seguida, edite-o.

Neste exemplo, é possível alterar a home page que é aberta quando um usuário final clica no botão **Abrir Navegador** no ambiente do Rescue and Recovery. A página da Web `http://www.lenovo.com/thinkvantage` é exibida.

Para fazer a alteração, quando o Notepad abrir com o arquivo PEACCESSIBMEN.INI:

1. Altere a linha:

   ```
   button13 = 8, "Open browser", 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__
   ```

   TO

   ```
   button13 = 8, "Open browser", Internet.bmp, 1, 1, 0,
   %sysdrive%\Preboot\Opera\Opera.EXE,
    http://www.ibm.com/thinkvantage
   ```

2. Coloque a nova versão na estrutura de diretórios para colocar os arquivos no ambiente do Rescue and Recovery. Para obter detalhes, consulte “Utilizando o RRUTIL.EXE” na página 20.
3. Reinicialize o sistema no ambiente do Rescue and Recovery.
4. Você fez algumas análises e determinou que existem arquivos cujos backups deverão ser feitos e outros que não precisam de backup, pois residem no servidor e podem ser obtidos após uma restauração do sistema. Para fazer isso, crie um arquivo IBMFILTER.TXT personalizado. Esse arquivo é colocado em um diretório com o arquivo NSF.CMD, que o copia para o local apropriado, conforme mostrado no exemplo a seguir:

   NSF.CMD:

   ```
   copy ibmfilter.txt "%RR%"
   ```

   IBMFILTER.TXT:

   ```
   x=*.nsf
   ```

Tabela 37. UPDATE_RR.CMD script

```
@ECHO OFF
::Obtain the PEAccessIBMen.ini file from the RR
c:\RRDeployGuide\RRUTIL\RRUTIL -g getlist.txt
c:\RRDeployGuide\GuideExample\RROriginal
:: Make a directory to put the edited file for import back into the RR
md c:\RRDeployGuide\GuideExample\put\preboot\usrintfc
:: Open the file with notepad and edit it.
ECHO.
ECHO Edit the file
c:\RRDeployGuide\GuideExample\RROriginal\PEAccessIBMen.ini

File will open automatically

pause
:: Make a copy of original file
copiar
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
:: Place the updated version of the PEAccessIBMen into the RR
c:\RRDeployGuide\RRUTIL\RRUTIL -p c:\RRDeployGuide\GuideExample\put
ECHO.
ECHO Reboot to the RR to see the change
pause
c:\Program Files\IBM ThinkVantage\Common\BMGR\bmgr32.exe /bw /r

Create GETLIST.TXT:

\preboot\usrintfc\PEAccessIBMen.ini
```

Instalando o Rescue and Recovery em Computadores Não-IBM

Para instalar o Rescue and Recovery, oito setores livres devem estar disponíveis no Registro de Inicialização Principal do disco rígido. O Rescue and Recovery utiliza um Gerenciador de Inicialização personalizado para entrar na área de Recuperação.

Alguns OEMs armazenam ponteiros para seus códigos de recuperação do produto no setor de Registro de Inicialização Principal. O código de recuperação do produto OEM pode interferir na instalação do Gerenciador de Inicialização do Rescue and Recovery.

Considere os seguintes cenários e as boas práticas para ajudar a garantir que o Rescue and Recovery forneça as funções e os recursos desejados:

Boas Práticas para a Configuração da Unidade de Disco Rígido: Cenário 1

Este cenário abrange implementações de nova imagem que incluem o Rescue and Recovery. Se implementar o Rescue and Recovery em clientes OEM existentes que contenham código de recuperação do produto OEM, execute o seguinte teste para determinar se o código de recuperação do produto OEM interfere no Rescue and Recovery:

1. Configure um cliente de teste com a imagem que contém o código de recuperação do produto OEM.

2. Instale o Rescue and Recovery. Se não houver oito setores livres no MBR resultantes do código de recuperação do produto OEM, você verá a seguinte mensagem de erro:

   ```
   Error 1722. There is a problem with this Windows
   Installer package. A program run as part of the
   setup did not finish as expected. Contact your
   personnel or package vendor.
   ```

Se você estiver utilizando uma imagem OEM do sistema operacional de base, assegure-se de que o Registro de Inicialização Principal não contenha os dados de recuperação do produto. Você pode fazer isso da seguinte maneira:

Atenção: A execução do comando a seguir apagará o conteúdo todo da unidade de disco rígido de destino. Depois de executá-lo, não será possível recuperar quaisquer dados da unidade de disco rígido de destino.

1. Utilize o arquivo CLEANDRV.EXE disponível na seção de ferramentas administrativas em:

   ```
   http://www.lenovo.com/ThinkVantage
   ```

   para garantir que o Registro de Inicialização Principal foi eliminado de todos os setores na unidade de disco rígido que você planeja utilizar para criar sua imagem básica.
2. Compacte a imagem de acordo com os procedimentos para implementação.

Boas Práticas para Configuração da Unidade de Disco Rígido: Cenário 2

A implementação do programa Rescue and Recovery em clientes existentes requer algum esforço e planejamento.

Se você receber o Erro 1722 e precisar criar oito setores livres, chame o help-desk da IBM para relatar o erro e obter instruções adicionais.

Criando um CD Inicializável do Rescue and Recovery

O Rescue and Recovery cria e grava um CD de mídia de recuperação a partir do conteúdo da área de serviço atual, em vez de a partir da imagem ISO pré-montada. Entretanto, se já existir uma imagem ISO apropriada, devido a ela já estar pré-carregada ou ter sido construída anteriormente, essa imagem será utilizada para gravar o CD, em vez de criar uma nova.

Devido aos recursos envolvidos, apenas uma instância do aplicativo de gravação do CD pode estar em execução em um determinado momento. Se ela estiver em execução, uma tentativa de iniciar uma segunda instância produzirá uma mensagem de erro e a segunda instância será interrompida. Além disso, devido à natureza de acesso a áreas protegidas da unidade de disco rígido, apenas administradores podem criar o ISO; entretanto, um usuário final limitado poderá gravar o ISO em um CD. Esses arquivos e diretórios serão incluídos no CD de recuperação:

- minint
- preboot
- win51
- win51ip
- win51ip.sp1

- scrrec.ver

Nota: Se você criar uma nova imagem ISO, deverá ter pelo menos 400 MB de espaço livre disponível na unidade do sistema para copiar as árvores de diretório e construir o ISO. A movimentação dessa grande quantidade de dados é intensa para a unidade de disco rígido e pode demorar 15 minutos ou mais em alguns computadores.

Criando o Arquivo ISO de Recuperação e Gravando no CD um Script de Arquivo de Amostra: Prepare o seguinte código:

```
:: Make an ISO file here - ISO will reside in c:\IBMTOOLS\rrcd
```

Nota: As sete linhas de código a seguir (em negrito) serão necessárias apenas se o sistema não for reincializado após a instalação.

```
:: Set up the environment
set PATH=%PATH%;%SystemDrive%\Program Files\IBM ThinkVantage\Common\Python24
set PATHEXT=%PATHEXT%;.PYW;.PYO;.PYC;.PY
set TCL_LIBRARY=%SystemDrive%\Program Files\IBM ThinkVantage\Common\Python24
\tcl\tcl8.4
set TK_LIBRARY=%SystemDrive%\Program Files\IBM ThinkVantage\Common\Python24
\tcl\tk8.4
set PYTHONCASEOK=1
set RR=c:\Program Files\IBM ThinkVantage\Rescue and Recovery\
set PYTHONPATH=C:\Program files\IBM ThinkVantage\Common\logger
:: The next line will create the ISO silently and not burn it
c:\Program Files\IBM ThinkVantage\Common\Python24\python c:\Program Files\
IBM ThinkVantage\Common\spi\mkspiim.pyc /scripted
:: The next line will create the ISO with user interaction and not burn it
:: c:\Program Files\IBM ThinkVantage\Common\Python24\python c:\Program Files\
IBM ThinkVantage\Common\spi\mkspiim.pyc /scripted
/noburn
```

Instalando o Rescue and Recovery em uma Partição de Serviço do Tipo 12

Você deve ter o seguinte para instalar o Rescue and Recovery em uma partição de serviço do tipo 12:
- O arquivo SP.PQI. Este arquivo inclui arquivos inicializáveis básicos para criar uma partição de serviço.
- PowerQuest PQDeploy.
- O instalador mais recente do Rescue and Recovery.

Há várias opções relacionadas à instalação do ambiente do Rescue and Recovery em uma partição de serviço.

Nota: A partição do tipo 12 deve residir na última entrada utilizada da tabela particionada na mesma unidade que contém o Windows, na unidade C:\. Você pode utilizar bmgr32 /info para determinar onde a partição do tipo 12 reside no HDD. Para obter informações adicionais, consulte “Controle do Gerenciador de Inicialização do Rescue and Recovery (BMGR32)” na página 162.

Para executar a instalação, conclua o seguinte procedimento:
1. Deixe pelo menos 700 MB de espaço livre não alocado no final da unidade.

2. Utilizando o PowerQuest, restaure o arquivo SP.PQI no espaço livre não alocado.
3. Exclua as partições principais criadas na etapa 1 (exceto a unidade C) e, em seguida, reinicialize.

   Nota: As informações sobre o volume do sistema podem estar na partição de serviço recém-criada. As informações sobre o volume do sistema devem ser excluídas por meio da Restauração do Sistema Windows.
4. Instale o Rescue and Recovery e reinicialize quando for solicitado.

Backup/Restauração de Sysprep

Observe que Persistência de Senha não funcionará com Backup/Restauração do Sysprep.

Você deve desativar e reinicializar o sistema depois de concluir um backup do Sysprep.

Computrace e Rescue and Recovery

Em sistemas não-BIOS, o Rescue and Recovery não poderá ser desinstalado se o Computrace estiver instalado.

Capítulo 9. Fingerprint Software

O console de impressão digital deve ser executado a partir da pasta de instalação do Fingerprint Software. A sintaxe básica é FPRCONSOLE [USER | SETTINGS]. O comando USER ou SETTINGS especifica qual conjunto de operações será utilizado. O comando completo será então, por exemplo, “fprconsole user add TestUser /FORCED”. Quando o comando não for conhecido ou nem todos os parâmetros estiverem especificados, a lista de comandos será mostrada junto com os parâmetros.

Para fazer download do Fingerprint Software e do Management Console, utilize o seguinte link

http://www.lenovo.com/think/support/site.wss/document.do?sitestyle=lenovo&indocid=TVAN-EAPFPR

Comandos Específicos do Usuário

A seção USER será utilizada para inscrever ou editar usuários. Quando o usuário atual não tiver direitos de administrador, o comportamento do console dependerá do modo de segurança do FS. Modo Conveniente: Os comandos ADD, EDIT e DELETE são possíveis para o usuário padrão. Entretanto, o usuário pode modificar apenas sua própria senha (inscrita com o seu nome de usuário). Modo de Segurança: nenhum comando é permitido. Sintaxe:

`FPRCONSOLE USER command`

em que *command* é um dos seguintes comandos: ADD, EDIT, DELETE, LIST, IMPORT, EXPORT.

Tabela 38.

Comando	Sintaxe	Descrição	Exemplo

Inscrever Novo Usuário	`ADD [username [| domain\ username]] [/FORCED]`	O sinalizador /FORCED desativará o botão Cancelar do assistente, de modo que a inscrição seja concluída com êxito. Se o nome do usuário não for especificado, então o nome do usuário atual será utilizado.	`fprconsole add domain0\testuser`
			`fprconsole add testuser`
			`fprconsole add testuser /FORCED`

Editar Usuário Inscrito	`EDIT [username [| domain\ username]]`	Se o nome do usuário não for especificado, então o nome do usuário atual será utilizado. **Nota:** O usuário editado deve verificar primeiro sua impressão digital.	`fprconsole edit domain0\testuser` `fprconsole edit testuser`

Tabela 38. (continuação)

Comando	Sintaxe	Descrição	Exemplo

Excluir um Usuário	`DELETE [username [| domain\ username | /ALL]]`	O sinalizador /ALL excluirá todos os usuários inscritos neste computador. Se o nome do usuário não for especificado, então o nome do usuário atual será utilizado.	`fprconsole delete domain0\testuser`
			`fprconsole delete testuser`
			`fprconsole delete /ALL`

Enumerar Usuários Inscritos	`List`		
Exportar Usuário Inscrito para um Arquivo	`Sintaxe: EXPORT username [| domain\username] file`	Este comando exportará um usuário inscrito para um arquivo da unidade de disco rígido. O usuário poderá então ser importado utilizando o comando IMPORT em outro computador ou no mesmo computador se o usuário for excluído.	
Importar Usuário Inscrito	`Sintaxe: IMPORT file`	A importação importará o usuário a partir do arquivo especificado. **Nota:** Se o usuário do arquivo já estiver inscrito no mesmo computador utilizando as mesmas impressões digitais, então não haverá garantia de qual usuário terá precedência na operação de identificação.	

Comandos de Configuração Global

As configurações globais do Fingerprint Software podem ser alteradas pela seção SETTINGS. Todos os comandos desta seção precisam de direitos de administrador. A sintaxe é:

`FPRCONSOLE SETTINGS command`

em que *command* é um dos seguintes comandos: SECUREMODE, LOGON, CAD, TBX, SSO.

Tabela 39.

Comando	Descrição	Sintaxe	Exemplo
Modo de Segurança	Esta configuração alterna entre o modo Conveniente e Segurança do Fingerprint Software.	`SECUREMODE 0|1`	Para configurar o modo conveniente: `fprconsole settings securemode 0`

Tabela 39. (continuação)

Comando	Descrição	Sintaxe	Exemplo
Tipo de Logon	Esta configuração ativa (1) ou desativa (0) o aplicativo de logon. Se o parâmetro /FUS for utilizado, o logon será ativado no modo Comutação Rápida de Usuário se a configuração do computador permitir.	`LOGON 0|1 [/FUS]`	
Mensagem CTRL+ALT+DEL	Esta configuração ativa(1) ou desativa(0) o texto "Pressionar CTRL+ALT+DEL" no logon.	`CAD 0|1`	
Segurança na Inicialização	Esta configuração desativa (0) globalmente o suporte à segurança na inicialização no Fingerprint Software. Quando o suporte à segurança na inicialização estiver desativado, nenhum assistente ou página de segurança na inicialização será mostrado e não importa quais sejam as configurações da BIOS.	`TBX 0|1`	
Conexão Única de Segurança na Inicialização	Esta configuração ativa(1) ou desativa(0) o uso de impressão digital utilizada no logon da BIOS para fazer logon automaticamente quando o usuário foi verificado na BIOS.	`SSO 0|1`	

Modo de Segurança vs. Conveniente

O ThinkVantage Fingerprint Software pode ser executado em dois modos de segurança, um modo conveniente e um modo de segurança.

O modo conveniente destina-se a computadores residenciais em que um nível de alta segurança não é tão importante. Todos os usuários podem executar todas as operações, incluindo a edição de senha de outros usuários e a possibilidade de efetuar logon no sistema utilizando senha (sem autenticação de impressão digital).

O modo de segurança destina-se a situações quando você deseja obter maior segurança. As funções especiais são reservadas apenas para administradores. Apenas administradores podem efetuar logon utilizando senha, sem autenticação adicional.

Um *Administrador* é qualquer membro do grupo Administradores local. Depois de definir o modo de segurança, apenas o administrador pode alterná-lo novamente para o modo simples.

Modo de Segurança – Administrador

No Logon, o Modo de Segurança exibirá a seguinte mensagem se um nome e uma senha de usuário errados forem digitados: ″Apenas administradores podem efetuar logon neste computador com o nome e a senha de usuário.″ Isso é feito para aprimorar a segurança e evitar fornecer informações a hackers sobre por que eles não conseguem efetuar logon.

Tabela 40.

Impressões Digitais	**Descrição**
Criar um Novo Passaporte	Os administradores podem criar seus próprios passaportes e podem criar também o passaporte de um usuário limitado.
Editar Passaportes	Os administradores podem editar *apenas* seus próprios passaportes.
Excluir Passaporte	Os administradores podem excluir todos os passaportes do usuário limitado e de outros administradores. Se outros usuários estiverem utilizando segurança na inicialização, o administrador terá a opção de remover gabaritos do usuário da segurança na inicialização, nesse momento.
Segurança na Inicialização	Os administradores podem excluir impressões digitais do Usuário Limitado e do Administrador utilizadas na inicialização. **Nota:** Deve haver pelo menos uma impressão digital presente quando o modo de inicialização estiver ativado.
Configurações	
Configurações de Logon	Os administradores podem fazer alterações em todas as configurações de logon.
Protetor de Tela Protegido	Os administradores podem acessar.
Tipo de Passaporte	Os administradores podem acessar - Relevante apenas com o servidor.
Modo de Segurança	Os administradores podem alternar entre os modos de Segurança e Conveniente.
Pró-servidores	Os administradores podem acessar - Relevante apenas com o servidor.

Modo de Segurança - Usuário Limitado

Durante um logon do Windows, um usuário Limitado deve utilizar uma impressão digital para efetuar logon. Se o leitor de impressão digital não estiver funcionando, um administrador precisará alterar a configuração do Fingerprint Software para o modo Conveniente para permitir o acesso do nome e senha do usuário.

Tabela 41.

Impressões Digitais	
Criar um Novo Passaporte	O usuário limitado não pode acessar.
Editar Passaportes	O usuário limitado pode editar apenas o seu próprio passaporte.
Excluir Passaporte	O usuário limitado pode excluir apenas o seu próprio passaporte.

Tabela 41. (continuação)

Impressões Digitais	
Segurança na Inicialização	O usuário limitado não pode acessar.
Configurações	
Configurações de Logon	O usuário limitado não pode modificar as configurações do Logon.
Protetor de Tela Protegido	O usuário limitado pode acessar.
Tipo de Passaporte	O usuário limitado não pode acessa.
Modo de Segurança	O usuário limitado não pode modificar os modos de segurança.
Pró-servidores	O usuário limitado pode acessar - Relevante apenas com o servidor.

Modo Conveniente - Administrador

Durante um logon do Windows, os administradores podem efetuar logon utilizando seu nome e senha de usuário ou sua impressão digital. .

Tabela 42.

Impressões Digitais	
Criar um Novo Passaporte	Os administradores podem criar *apenas* o seu próprio passaporte
Editar Passaportes	Os administradores podem editar *apenas* seus próprios passaportes.
Excluir Passaporte	Os administradores podem excluir *apenas* os seus próprios passaportes.
Segurança na Inicialização	Os administradores podem excluir impressões digitais do Usuário Limitado e do Administrador utilizadas na inicialização. **Nota:** Deve haver pelo menos uma impressão digital presente quando o modo de inicialização estiver ativado.
Configurações	
Configurações de Logon	Os administradores podem fazer alterações em todas as configurações de logon.
Protetor de Tela Protegido	Os administradores podem acessar.
Tipo de Passaporte	Os administradores podem acessar - Relevante apenas com o servidor.
Modo de Segurança	Os administradores podem alternar entre os modos de Segurança e Conveniente.
Pró-servidores	Os administradores podem acessar - Relevante apenas com o servidor.

Modo Conveniente - Usuário Limitado

Durante um logon do Windows, os usuários limitados podem efetuar logon utilizando seu nome e senha de usuário ou sua impressão digital.

Tabela 43.

Impressões Digitais	
Criar um Novo Passaporte	Os usuários limitados podem criar apenas sua própria senha.
Editar Passaportes	Os usuários limitados podem editar apenas seu próprio passaporte
Excluir Passaporte	Os usuários limitados podem excluir apenas o seu próprio passaporte
Segurança na Inicialização	Os usuários limitados podem excluir apenas suas próprias impressões digitais.
Configurações	
Configurações de Logon	Os usuários limitados não podem modificar as configurações do Logon
Protetor de Tela Protegido	Os usuários limitados podem acessar
Tipo de Passaporte	Os usuários limitados não podem acessar - Relevante apenas com o servidor
Modo de Segurança	Os usuários limitados não podem modificar os modos de segurança
Pró-servidores	Os usuários limitados podem acessar - Relevante apenas com o servidor.

ThinkVantage Fingerprint Software e Novell Netware Client

Os nomes e senhas de usuários do ThinkVantage Fingerprint Software e Novell devem coincidir.

Se você tiver o ThinkVantage Fingerprint Software instalado no computador e, em seguida, instalar o Novell Netware Client, alguns itens do registro poderão ser sobrescritos. Se você tiver problemas com o logon do ThinkVantage Fingerprint Software, vá para a tela de configurações do Logon e reative o Protetor de Logon.

Se você tiver o Novell Netware Client instalado no computador, mas não tiver efetuado logon no cliente antes de instalar o ThinkVantage Fingerprint Software, a tela de Logon do Novell será exibida. Forneça as informações solicitadas pela tela.

Para alterar as Configurações do Protetor de Logon:

- Inicie o Centro de Controle.
- Clique em **Configurações**
- Clique em **Configurações de Logon**
- Ative ou desative o Protetor de Logon.

  Se você deseja utilizar logon de impressão digital, marque a caixa de opções Substituir logon do Windows por logon protegido com impressão digital. Observe que a ativação e a desativação do protetor de logon requer uma reinicialização.
- Ative ou desative a comutação rápida do usuário, quando suportada pelo sistema.
- (Recurso opcional) Ative ou desative o logon automático de um usuário autenticado pela segurança na inicialização.
- Defina as configurações de Logon da Novell. As seguintes configurações estão disponíveis ao efetuar logon em uma rede Novell:

– **Ativada**

  O ThinkVantage Fingerprint Software fornece automaticamente credenciais conhecidas. Se o logon da Novell falhar, a tela de logon do Novell Client será exibida juntamente com um prompt para digitar os dados corretos.

– **Perguntar durante logon**

  O ThinkVantage Fingerprint Software exibe a tela de logon do Novell Client e um prompt para digitar os dados de logon.

– **Desativado**

  O ThinkVantage Fingerprint Software não tenta efetuar um logon da Novell.

Apêndice A. Parâmetros de Linha de Comandos de Instalação

O Microsoft Windows Installer fornece várias funções de administrador por meio de parâmetros de linha de comandos.

Procedimento de Instalação Administrativa e Parâmetros de Linha de Comandos

O Windows Installer pode executar uma instalação administrativa de um aplicativo ou produto em uma rede para ser utilizado por um grupo de trabalho ou para personalização. No pacote de instalação do Rescue and Recovery, uma instalação administrativa descompacta os arquivos de origem de instalação em um local especificado.

- Para executar uma instalação administrativa, execute o pacote de instalação na linha de comandos utilizando o parâmetro /a:

  ```
  Setup.exe /a
  ```

A instalação administrativa apresenta um assistente que solicita que o usuário administrativo especifique os locais para descompactação dos arquivos de instalação. O local padrão para extração é C:\. Você pode escolher um novo local que pode incluir unidades diferentes de C:\ (outras unidades locais, unidades de rede mapeadas, etc.). Também é possível criar novos diretórios durante esta etapa.

- Para executar uma instalação administrativa silenciosamente, você pode definir a propriedade pública TARGETDIR na linha de comandos para especificar o local de extração:

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

  Ou

  ```
  msiexec.exe /i "IBM Rescue and Recovery.msi" /qn TARGERDIR=F:\IBMRR
  ```

Depois de concluir a instalação administrativa, o administrador pode personalizar os arquivos de origem, como adicionar configurações a TVT.TXT.

Utilizando MSIEXEC.EXE

Para instalar a partir da origem descompactada depois de fazer personalizações, o usuário deverá chamar MSIEXEC.EXE da linha de comandos, transmitindo o nome do arquivo *.MSI descompactado. MSIEXEC.EXE é o programa executável do Installer utilizado para interpretar pacotes de instalação e instalar produtos nos sistemas de destino.

```
msiexec /i "C:\WindowsFolder\Profiles\UserName\
Personal\MySetups\nome_do_projeto\configuração_do_produto\nome_do_release\
DiskImages\Disk1\nome_do_produto.msi"
```

Nota: Digite o comando acima em uma única linha, sem espaços após as barras. A Tabela 44 na página 138 descreve os parâmetros de linha de comandos disponíveis que podem ser utilizados com MSIEXEC.EXE e exemplos de como utilizá-los.

Tabela 44. Parâmetros de Linha de Comandos

Parâmetro	Descrição
/I *pacote* ou *código do produto*	Utilize este formato para instalar o produto: `Othello:msiexec /i "C:\WindowsFolder\Profiles\UserName\Personal\MySetups\Othello\Trial Version\Release\DiskImages\Disk1\Othello Beta.msi"` O código do produto refere-se ao GUID que é gerado automaticamente na propriedade do código do produto da visualização do seu projeto de produto.
/a *pacote*	A opção **/a** permite que os usuários com privilégios de administrador instalem um produto na rede.
/x *pacote* ou *código do produto*	A opção **/x** desinstala um produto.
/L [i|w|e|a|r|u|c|m|p|v|+] *arquivo de log*	A construção com a opção **/L** especifica o caminho para o arquivo de log; esses sinalizadores indicam quais informações registrar no arquivo de log: • **i** registra mensagens de status • **w** registra mensagens de aviso não fatais • **e** registra todas as mensagens de erro • **a** registra o início das seqüências de ações • **r** registra registros específicos da ação • **u** registra pedidos do usuário • **c** registra parâmetros da interface com o usuário inicial • **m** registra mensagens de falta de memória • **p** registra configurações do terminal • **v** registra configuração de saída prolixa • **+** anexa a um arquivo existente • * é um caractere curinga que permite registrar todas as informações (exceto a configuração de saída prolixa)
/q [n|b|r|f]	A opção /q é utilizada para definir o nível da interface com o usuário, juntamente com os seguintes sinalizadores: • **q** ou qn não cria uma interface com o usuário • **qb** cria uma interface com o usuário básica As configurações de interface com o usuário a seguir exibem uma caixa de diálogo modal no final da instalação: • **qr** exibe uma interface com o usuário reduzida • **qf** exibe uma interface com o usuário completa • **qn+** não exibe uma interface com o usuário • **qb+** exibe uma interface com o usuário básica
/? ou /h	Qualquer um dos comandos exibe informações de copyright do Windows Installer.

Tabela 44. Parâmetros de Linha de Comandos (continuação)

Parâmetro	Descrição

TRANSFORMS	Utilize o parâmetro de linha de comando **TRANSFORMS** para especificar quaisquer transformações que você gostaria de aplicar em seu pacote básico. A chamada da linha de comandos de transformação pode se assemelhar a esta:
	`msiexec /i "C:\WindowsFolder\`
	`Profiles\UserName\Personal`
	`\MySetups\`
	`Nome_do_seu_Projeto\Versão_de_Teste\`
	`Meu Release-1`
	`\DiskImages\Disk1\`
	`ProductName.msi" TRANSFORMS="New Transform 1.mst"`
	
	Você pode separar várias transformações com um ponto-e-vírgula. Portanto, recomenda-se não utilizar ponto-e-vírgula no nome da transformação, pois o serviço do Windows Installer os interpretará de maneira incorreta.

Propriedades	Todas as propriedades públicas podem ser definidas ou modificadas a partir da linha de comandos. As propriedades públicas se distinguem das propriedades privadas por estarem em letras maiúsculas. Por exemplo, *COMPANYNAME* é uma propriedade pública.
	
	Para definir uma propriedade a partir da linha de comandos, utilize a seguinte sintaxe:
	`PROPERTY=VALUE`
	
	Se você deseja alterar o valor de *COMPANYNAME*, deverá digitar o seguinte:
	`msiexec /i "C:\WindowsFolder\`
	`Profiles\UserName\Personal`
	`\`
	`MySetups\Nome_do_seu_Projeto\`
	`Versão_de_Teste\Meu Release-1`
	`\`
	`DiskImages\Disk1\ProductName.msi"`
	`COMPANYNAME="InstallShield"`

Apêndice B. Configurações e Valores do TVT.TXT

Os valores padrão a seguir são as configurações sugeridas. Os valores podem ser diferentes para configurações diferentes, Pré-carga, Download da Web e versão OEM, por exemplo. As seguintes definições de configuração de instalação estão disponíveis:

Tabela 45. Configurações e valores do TVT.TXT

Configuração	Valores
AccessFile (consulte GUIGroup)	*nome do arquivo*, em que *nome do arquivo* é o caminho completo para um arquivo que contém os nomes dos grupos locais (não grupos de domínio) do Windows que são permitidos para executar operações do Rescue and Recovery. Se houver espaços em branco ou ausentes, todos os usuários que puderem efetuar login no computador poderão ativar a GUI e executar operações de linha de comandos. Por padrão, o arquivo está em branco.
BackupPartition	0 = Primeira partição em uma unidade especificada. 1 = Segunda partição em uma unidade especificada. 2 = Terceira partição em uma unidade especificada. 3 = Quarta partição em uma unidade especificada. As unidades são especificadas nas seguintes seções: [BackupDisk] = unidade de disco rígido local. [SecondDisk] = segunda unidade de disco rígido local. [USBDisk] = unidade de disco rígido USB. **Nota:** As partições já devem existir. Caso contrário, o usuário será solicitado a estabelecer a partição (se houver mais de uma partição na unidade de destino quando a unidade de destino for selecionada na interface com o usuário).
BatteryPercentRequired	O intervalo é de 0 a 100. O padrão é 100.
CPUPriority	*n* em que *n* = 1 a 5; 1 é a prioridade mais baixa e 5 é a prioridade mais alta. O padrão é 3.
CustomPartitions	0 = Fazer backup de todas as partições. 1 = Examinar IncludeInBackup em cada partição.
DisableAnalyze	0 = Mostrar opção Otimizar armazenamento de backup. 1 = Ocultar essa opção. O padrão é 0.
DisableArchive	0 = Ativar archive. 1 = Ocultar archive. O padrão é 0.

Tabela 45. Configurações e valores do TVT.TXT (continuação)

Configuração	Valores
DisableBackupLocation	0 = Ativar todos os destinos. 0x01 = Desativar o destino local. 0x02 = Desativar a unidade Cd/DVD. 0x08 = Desativar USB/ unidade de disco rígido. 0x10 = Desativar rede. 0x20 = Desativar a segunda unidade de disco rígido. 1 = Ocultar archive. Esses podem ser combinados para desativar vários locais. Por exemplo, um valor de 0x0A poderia desativar o CD/DVD e a unidade de disco rígido USB, um valor de 0x38 poderia desativar a unidade de disco rígido USB, a rede e a segunda unidade de disco rígido. Para ativar apenas o backup da unidade de risco rígido local, você pode utilizar 0x3A (ou mesmo 0xFE)).
DisableBootDisc	0 = Criar CD inicializável ao criar backups de CD/DVD. 1 = Não criar CD inicializável. A função Desativar Disco de Inicialização é apenas para Backups que não sejam Archive.
DisableDelete	0 = Mostrar opção excluir backups. 1 = Ocultar essa opção. O padrão é 0.
DisableExclude	0 = Mostrar opção excluir arquivo/pastas. 1 = Ocultar essa opção. O padrão é 0.
DisableLiveUpdate	0 = Mostrar opção LiveUpdate. 1 = Ocultar essa opção. O padrão é 0.
DisableMigrate	0 = Mostrar criar arquivo de migração a partir do backup. 1 = Ocultar essa opção. O padrão é 0.
DisableRestore	0 = Ativar restauração. 1 = Ocultar restauração. O padrão é 0.
DisableSchedule	0 = Mostrar opção planejamento de backup. 1 = Ocultar opção planejamento de backup. O padrão é 0.

Tabela 45. Configurações e valores do TVT.TXT (continuação)

Configuração	Valores
DisableSFR	0 = Ativar restauração de arquivo simples. 1 = Ocultar restauração de arquivo simples. O padrão é 0.
DisableSingleStorage	0 = Mostrar opção de armazenamento único. 1 = Ocultar essa opção. O padrão é 0.
DisableViewBackups	0 = Mostrar opção visualizar backups. 1 = Ocultar essa opção. O padrão é 0.
DisableVerifyDisc	0 = Verificar operações de gravação óptica. 1 = Não verificar operações de gravação óptica. O padrão é 0.
Exclude (consulte Include)	0 = Não aplicar GUIEXCLD.TXT. 1 = Aplicar GUIEXCLD.TXT.txt. **Notas:** 1. Exclude e Selecionar arquivos podem ser definidos antes da instalação e podem ser aplicados durante o processo de instalação. 2. Exclude e Include não podem ser 1.
GUIGroup (consulte AccessFile)	*grupo*, em que *grupo* é um grupo local (não um grupo de domínio) do Windows que é permitido para executar operações do Rescue and Recovery. A lista de grupos privilegiados é armazenada em um arquivo definido pela entrada AccessFile.
HideAdminBackups	0 = Mostrar backups do administrador na lista. 1 = Ocultar backups do administrador. O padrão é 0.
HideBaseFromDelete	0 = Mostrar o backup básico no diálogo Excluir Backups. 1 = Ocultar backup básico no diálogo Excluir Backups. O padrão é 0.
HideBootUSBDialog	0 = Mostrar aviso se estiver fazendo backup para uma unidade de disco rígido USB e ela não for inicializável 1 = Ocultar aviso O padrão é 0.
HideDiffFileSystems	0 = Mostrar partições FAT/FAT32 ao restaurar/salvar arquivos 1 = Ocultar partições FAT/FAT32 ao restaurar/salvar arquivos O padrão é 0.

Tabela 45. Configurações e valores do TVT.TXT (continuação)

Configuração	Valores
HideCSSEncrypt	0 = Não ocultar Criptografar backups usando o Client Security Solution 1 = Ocultar Criptografar backups usando o Client Security Solution O padrão é 0.
HideGUI	0 = Mostrar a GUI para usuários autorizados 1 = Ocultar a GUI de todos os usuários
HideLocationNotFoundMessage	0 = Mostrar a mensagem do diálogo 1 = Ocultar a mensagem do diálogo O padrão é 0.
HideLockHardDisk	0 = Mostrar a opção proteger disco rígido contra corrupção do MBR 1 = Ocultar essa opção O padrão é 1.
HideMissedBackupMessages	0 = Mostrar caixa de diálogo 1 = Ocultar caixa de diálogo O padrão é 1.
HideNoBatteryMessage	0 = Exibir mensagem 1 = Ocultar mensagem O padrão é 1
HideNumBackupsDialog	0 = Não ocultar o diálogo que mostra ao usuário que ele atingiu o número máximo de backups 1 = Ocultar o diálogo que mostra ao usuário que ele atingiu o número máximo de backups O padrão é 1
HidePowerLossBackupMessage	0 = Mostrar mensagem de perda de força com backup 1 = Ocultar mensagem O padrão é 0.
HidePasswordPersistence	0 = Ocultar GUI 1 = Mostrar GUI O padrão é 0.
HidePasswordProtect	0 = Mostrar caixa de opções protegida por senha. 1 = Ocultar caixa de opções protegida por senha. O padrão é 0.

Tabela 45. Configurações e valores do TVT.TXT (continuação)

Configuração	Valores
HideSuspendCheck	0 = Não ocultar a caixa de opções despertar o computador de suspensão/hibernação. 1 = Ocultar a caixa de opções. O padrão é 1.
Incluir (consulte Exclude)	0 = Não aplicar GUIINCLD.TXT. 1 = Aplicar GUIINCLD.TXT e exibir a opção para definir arquivos e pastas include. **Notas:** 1. Exclude e Selecionar arquivos podem ser definidos antes da instalação e podem ser aplicados durante o processo de instalação. 2. Exclude e Include não podem ser 1.
LocalBackup2Location	*x**nome da pasta* em que *x* = a letra da unidade e *nome da pasta* é qualquer nome completo de pasta). O padrão é este: *Letra da primeira partição na segunda unidade*:\IBMBackupData **Notas:** 1. Como a letra da unidade pode ser alterada em algum momento, o Rescue and Recovery associará a letra da unidade a uma partição no momento da instalação e, em seguida, utilizará as informações sobre a partição em vez da letra da unidade. 2. Este é o campo de local da entrada `TaskParameters`.
LockHardDisk	0 = Não bloquear o disco rígido para proteger o MBR. 1 = Bloquear o disco rígido. O padrão é 0.
MaxBackupSizeEnforced	*x*, em que *x* é o tamanho em GB. Este valor não impedirá que um backup exceda esse limite. Entretanto, se o limite for excedido, o usuário será avisado sobre o tamanho do arquivo na próxima vez em que um backup ″On Demand″ for feito.O padrão é 0.
MaxNumberOf IncrementalBackups	padrão = 5, mín = 2, máx = 32
MinAnalyzeFileSize *n*	Em que *n* é o tamanho mínimo de arquivo em MB para exibir um arquivo ao usuário na tela ″Otimizar espaço de armazenamento de backup″. O padrão é 20
NetworkUNCPath	Compartilhamento de rede utilizando o formato: *\\nome do computador\sharefolder* Não há padrão. **Nota:** Este local não será protegido pelo Driver de Filtro de Arquivo.
NetworkUNCPath	*nome de compartilhamento do servidor*, por exemplo, \\MYSERVER\SHARE\FOLDER
NumMinutes	*x*, em que a tarefa é executada depois de *x* minutos.

Tabela 45. Configurações e valores do TVT.TXT (continuação)

Configuração	Valores
PasswordRequired	0 = Nenhuma senha requerida para abrir o ambiente do Rescue and Recovery. 1 = Senha requerida para abrir o ambiente do Rescue and Recovery.
PDAPreRestore	*cmd*, em que *cmd* é o caminho completo para o programa ser executado no ambiente do Rescue and Recovery, antes de uma operação de restauração.
PDAPreRestore *n*	*cmd*, em que *cmd* é o caminho completo para o programa ser executado no ambiente do Rescue and Recovery, antes de uma operação de restauração.
PDAPreRestoreParameters	Os parâmetros a serem utilizados no programa PDARestore.
PDAPreRestoreParameters *n*	Os parâmetros a serem utilizados no programa PDARestore.
PDAPreRestoreShow	0 = Ocultar tarefa. 1 = Mostrar tarefa.
PDAPreRestoreShow *n*	0 = Ocultar tarefa. 1 = Mostrar tarefa.
PDAPostRestore	*cmd*, em que *cmd* é o caminho completo para o programa ser executado no ambiente do Rescue and Recovery, antes de uma operação de restauração.
PDAPostRestore *n*	*cmd*, em que *cmd* é o caminho completo para o programa ser executado no ambiente do Rescue and Recovery, antes de uma operação de restauração.
PDAPostRestoreParameters	Os parâmetros a serem utilizados no programa PDARestore.
PDAPostRestoreParameters *n*	Os parâmetros a serem utilizados no programa PDARestore.
PDAPostRestoreShow	0 = Ocultar tarefa. 1 = Mostrar tarefa.
PDAPostRestoreShow *n*	0 = Ocultar tarefa. 1 = Mostrar tarefa.
Post (consulte PostParameters)	*cmd*, em que *cmd* é o caminho completo para um arquivo executável ser executado após a tarefa principal.
Post (consulte PostParameters) *n*	Em que *n* é o número do backup 0, 1, 2, 3...32 *cmd*, em que *cmd* é o caminho completo para um arquivo executável ser executado após a tarefa principal. Por exemplo: • Post0=command.bat *path* Este é executado após o backup básico • Post1=command.bat *path* Este é executado após o backup incremental **Nota:** Isto é apenas para Backup
PostParameters (consulte Post)	*cmd*, em que *cmd* é o caminho completo para um arquivo executável ser executado após a tarefa principal. Isto é apenas para Backup.

Tabela 45. Configurações e valores do TVT.TXT (continuação)

Configuração	Valores
PostParameters *n* (consulte Post)	*parms*, em que *parms* são parâmetros a serem utilizados na tarefa de envio
	parms, em que *parms* são parâmetros a serem utilizados na tarefa de envio. **Nota:** Isto é apenas para Backup
PostRestore	*cmd*, em que *cmd* é o caminho completo para o programa ser executado no Windows depois de a operação de restauração ser concluída.
PostRestore *n*	*cmd*, em que *cmd* é o caminho completo para o programa ser executado no Windows depois de a operação de restauração ser concluída.
PostRestoreParameters	Os parâmetros a serem utilizados no programa PostRestore
PostRestoreParameters *n*	Os parâmetros a serem utilizados no programa PostRestore
PostRestoreShow	0 = Ocultar tarefa de restauração. 1 = Mostrar tarefa de restauração.
PostRestoreShow *n*	0 = Ocultar tarefa de restauração. 1 = Mostrar tarefa de restauração.
PostShow	0 = Ocultar tarefa de envio. 1 = Mostrar tarefa de envio. O padrão é 0.
PostShow *n*	0 = Ocultar tarefa de envio. 1 = Mostrar tarefa de envio. O padrão é 0. Em que *n* é o número do backup 0, 1, 2, 3....32 **Nota:** Isto é apenas para Backup
Pre (consulte PreParameters)	*cmd*, em que *cmd* é o caminho completo para um arquivo executável ser executado antes da tarefa principal.
Pre (Consulte PreParameters) *n*	Em que *n* é o número do backup 0, 1, 2, 3....32 *cmd*, em que *cmd* é um caminho completo para um arquivo executável a ser executado antes da tarefa primária. Por exemplo: • Pre0=command.bat *path* Este é executado antes do backup básico • Pre1=command.bat *path* Este é executado antes do backup incremental **Nota:** Isto é apenas para Backup.
PreParameters (consulte Pre)	Em que *parms* são os parâmetros a serem utilizados para a pré-tarefa
PreRejuvenate *cmd*	Em que *cmd* é o caminho completo para o programa a ser executado no Windows antes de uma operação de renovação
PreRejuvenateParameters *parms*	Em que *parms* são os parâmetros a serem utilizados no programa PreRejuvenate.

Tabela 45. Configurações e valores do TVT.TXT (continuação)

Configuração	Valores
PreRejuvenateShow	0 = Ocultar tarefa. 1 = Mostrar tarefa.
PostRejuvenate *cmd*	*cmd*, em que *cmd* é o caminho completo para o programa ser executado no Windows após uma operação de renovação.
PostRejuvenateParameters *parms*	Em que *parms* são os parâmetros a serem utilizados no programa PostRejuvenate.
PostRejuvenateShow	0 = Ocultar tarefa. 1 = Mostrar tarefa.
PreShow	0 = Ocultar pré-tarefa. 1 = Mostrar pré-tarefa. O padrão é 1.
PreShow *n*	Em que *n* é o número do backup 0, 1, 2, 3....32. *cmd*, em que *cmd* é um caminho completo para um arquivo executável a ser executado antes da tarefa primária. **Nota:** Isto é apenas para Backup
PreWinRestore	*cmd*, em que *cmd* é o caminho completo para o programa ser executado no Windows, antes de uma operação de restauração.
PreWinRestore *n*	*cmd*, em que *cmd* é o caminho completo para o programa ser executado no Windows, antes de uma operação de restauração.
PreWinRestoreParameters	Os parâmetros a serem utilizados no programa PreWinRestore.
PreWinRestoreParameters *n*	Os parâmetros a serem utilizados no programa PreWinRestore.
PreWinRestoreShow	0 = Ocultar tarefa de envio. 1 = Mostrar tarefa de envio.
PreWinRestoreShow *n*	0 = Ocultar tarefa de envio. 1 = Mostrar tarefa de envio.
ResumePowerLossBackup	0 = Não retomar o processo de backup se tiver havido uma queda de energia no meio do último backup. 1 = Retomar o backup. O padrão é 1.

Tabela 45. Configurações e valores do TVT.TXT (continuação)

Configuração	Valores
RunBaseBackup	0 = Não fazer o backup básico. 1 = Fazer o backup básico. O padrão é 0. `runbasebackuplocation=(Local)` Os valores são: L = Local U = USB N = Rede S = Segundo HDD C = CD
ScheduleDayOfTheMonth	*x*, em que *x* é igual a 1 a 28 ou 35 apenas para backups mensais. 35 = o último dia do mês.
ScheduleDayOfTheWeek	Apenas para backups semanais. 0 = Domingo 1 = Segunda-feira 2 = Terça-feira 3 = Quarta-feira 4 = Quinta-feira 5 = Sexta-feira 6 = Sábado O padrão é 0 (Domingo).
ScheduleFrequency	0 = Não planejado 1 = Diariamente 2 = Semanalmente 3 = Mensalmente O padrão é 2 (semanalmente).
ScheduleHour	*x*, em que *x* é igual a 0 a 23 e 0 é 12:00 AM, 12 é meio dia e 23 é 11:00 PM. O padrão é 0.
ScheduleMinute	*x*, em que *x* é igual a 0 a 59 (que aumenta) que representa o minuto na hora para iniciar o backup incremental. O padrão é 0.

Tabela 45. Configurações e valores do TVT.TXT (continuação)

Configuração	Valores
ScheduleWakeForBackup	0 = Não ativar o computador para backups planejados. 1 = Ativar o computador, se ele for um desktop para backups planejados, mas não ativar computadores portáteis. 2 = Ativar o computador, independentemente de ser um desktop ou um computador portátil. O padrão é 2. **Nota:** Se um computador portátil ativar um backup, mas a alimentação ac não for detectada, ele voltará ao modo de suspensão/hibernação antes de a operação de backup ser iniciada.
ScheduleMode	*x*, em que *x* é uma máscara de bits com um valor de: • 0 = Sem planejamento • 0x01 = A cada minuto • 0x04 = Todas as semanas • 0x08 = Todos os meses • 0x10 = Sempre que o serviço for iniciado (normalmente a cada inicialização da máquina) • 0x20 = A máquina sai da suspensão/hibernação • 0x40 = A unidade de disco rígido USB se torna conectada • 0x80 = A rede se torna conectada • 0x100 = A rede se torna desconectada • 0x200 = Reconfiguração da senha do BIOS • 0x400 = Substituição da placa-mãe Este parâmetro é atualizado automaticamente quando o usuário altera os valores da GUI. Se o valor ScheduleFrequency for alterado manualmente para o arquivo ou o script TVT.TXT, reloadsched atualizará este parâmetro. **Nota:** Os bits da `Unidade de disco rígido USB se torna conectada` ou de `A rede se torna conectada` não precisam ser definidos para sincronização automática de backups da unidade de disco rígido local para unidade de disco rígido USB ou rede).
SkipLockedFiles	0 = Exibir caixa de diálogo quando um arquivo bloqueado e corrompido for encontrado. 1 = Sempre ignorar arquivos bloqueados e corrompidos.
SPBackupLocation=2	Usado para configurar o backup da Partição de Serviço. Se esta configuração não for usada, a Partição de Serviço padrão de 500 MB será restaurada ao inicializar o CD, restaurando o CD e outros dados da Partição de Serviço serão removidos.
Task	*cmd*, em que *cmd* é um caminho completo para o programa ser executado como a tarefa principal. **Nota:** O número de tarefas não pode ser mais que 50.
TaskParameter	*parms* são parâmetros a serem utilizados na tarefa.
TaskShow	0 = Ocultar tarefa 1 = Mostrar tarefa O padrão é 0.

Tabela 45. Configurações e valores do TVT.TXT (continuação)

Configuração	Valores
UUIDMatchRequired	0 = A correspondência de UUID do computador não é obrigatória. 1 = A correspondência de UUID do computador é obrigatória. **Nota:** Os backups capturados quando UUIDMatchRequired foi definido como 1 continuarão a exigir uma correspondência de UUID, mesmo se essa definição for alterada posteriormente.
Yield	*n* em que *n* é igual a 0 a 8; 0 significa que o Rescue and Recovery não produz e 8 significa que o Rescue and Recovery produz o valor máximo de rendimento. **Nota:** Um rendimento mais alto diminuirá de forma incremental o desempenho do backup e fornecerá melhor desempenho interativo. O padrão é 0.

Depois que o Rescue and Recovery for instalado, as seguintes configurações poderão ser alteradas no arquivo TVT.TXT que está localizado no diretório instalado. Elas serão inicializadas com os valores designados durante a instalação.

Backup e Restauração do TVT.txt

A fim de suportar a instalação silenciosa, a configuração de Backup e Restauração do Rescue and Recovery é definida por um arquivo externo (*TVT.TXT*) que é editado antes da instalação. O arquivo TVT.TXT seguirá o formato de arquivo padrão do Windows .ini, com os dados organizados por seção, mostrados entre [] e uma entrada por linha no formato “setting=value”. O Rescue and Recovery utilizará o nome do produto como o cabeçalho da seção (como Rapid Restore Ultra). Além disso, o arquivo de filtro include/exclude pode ser definido antes da instalação e ser aplicado durante o processo de instalação.

Se o administrador de TI quiser personalizar seus backups com configurações, deverá editar o arquivo txt.txt no diretório de instalação. O melhor momento para fazer isso é antes da instalação do Rescue and Recovery ou depois da instalação e antes do primeiro backup. Um arquivo TVT.TXT está incluído em cada local de backup. Antes do primeiro backup, há apenas um arquivo TVT.TXT. Se essa abordagem for utilizada, todos os backups serão alterados sem quaisquer problemas de versão e de sincronização do TVT.TXT. Às vezes, o arquivo TVT.TXT precisará ser editado após um backup. Nesse caso, há duas maneiras de atualizar todos os arquivos TVT.TXT com as últimas alterações. O administrador de TI pode copiar o arquivo TVT.TXT do diretório de instalação para todas as pastas de backup ou iniciar outro backup e o processo sincronizará automaticamente todas as versões do TVT.TXT com a versão do diretório de instalação. O segundo método é preferível.

Planejando Backups e Tarefas Associadas

O planejador não foi projetado para ser específico ao Rescue and Recovery. Entretanto, a configuração é armazenada no mesmo arquivo TVT.TXT. Quando o Rescue and Recovery for instalado, ele preencherá o planejador com as configurações apropriadas.

Segue uma descrição da estrutura do planejador:

- Local: Pasta de instalação.
- Entrada para cada job planejado.
- Script a ser executado.
- Named pipe a ser utilizado para notificações de progresso. Isso é opcional.
- Informações sobre vários planejamentos mensais, semanais, diários, nos dias úteis, nos fins de semana; às terças e sextas, por exemplo, pode ser suportado criando-se dois planejamentos.
- Variáveis a serem transmitidas para as funções.

Considere o seguinte exemplo: No caso de o Rescue and Recovery executar backup incremental no planejamento, com callbacks antes e depois do backup, a seguinte entrada instrui o aplicativo adequadamente:

```
[SCHEDULER]
Task1=rescuerecovery
[rescuerecovery]
Task="c:\Arquivos de
programas\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:\Arquivos de programas\antivirus\scan.exe"
Post="c:\Arquivos de programas\logger\log.bat"
```

Gerenciando Arquivos TVT.txt Diferentes

Como as unidades de disco rígido podem ter várias partições, o programa de backup e restauração precisa saber em qual partição armazenará os dados de backup. Se um determinado destino tiver várias partições e as operações de backup forem colocadas em scripts, as seguintes definições deverão ser configuradas antes da operação de backup. Se a operação de backup puder ser iniciada pelo usuário, você poderá ignorar esta seção.

Para backups na unidade de disco rígido local, a definição de configuração estará localizada no arquivo TVT.TXT, na seção BackupDisk. Os backups na segunda unidade de disco rígido local utilizam a seção SecondDisk e os backups na unidade de disco rígido USB utilizam a seção USBDisk, conforme mostrado:

```
BackupPartition=x
```

em que *x* é um intervalo de 0 a 3, em que 0 representa a primeira partição na unidade apropriada.

Nota: As partições já devem existir. Caso contrário, o usuário será avisado, se houver mais de uma partição, quando o destino apropriado for selecionado na GUI. Por exemplo: se precisar fazer backup na segunda partição da unidade de disco rígido USB, então a entrada de arquivo TVT.TXT se assemelhará a isto:

```
[USBDisk]
BackupPartition=1
```

Mapeando uma Unidade de Rede para Backups

A função mapear unidade de rede depende do arquivo MAPDRV.INI localizado no diretório C:\Arquivos de programas\IBM ThinkVantage\Common\MND. Todas as informações são armazenadas na seção DriveInfo.

A entrada Convenção Universal de Nomenclatura contém o nome do computador e compartilha o local ao qual você está tentando se conectar.

A entrada NetPath é emitida a partir do mapdrv.exe. Ela contém o nome real que foi utilizado ao estabelecer a conexão.

As entradas User e Pwd são as entradas de nome de usuário e senha. Elas são criptografadas.

Segue uma entrada de exemplo para mapeamento de uma unidade de rede:

```
[DriveInfo]
UNC=\\server\share
NetPath=\\9.88.77.66\share
User=116226064151192077230149185054220105210064012092037082020 15...
Pwd=11622606415100000000014918505422010521006401209203708202015...
```

Na implementação, esse arquivo pode ser copiado em vários computadores que utilizarão o mesmo nome de usuário e a mesma senha. A entrada UNC é sobrescrita pelo Rapid Restore Ultra, com base em um valor do TVT.TXT.

Configurando Contas de Usuário para Backups de Rede

Quando o diretório RRBACKUPS é criado no compartilhamento de rede, o serviço torna o diretório uma pasta de leitura e designa a ela direitos de acesso para que *apenas* a conta que criou a pasta tenha controle total sobre a pasta.

Para concluir uma operação de mesclagem, as permissões MOVE devem existir para a conta User. Se tiver efetuado login com uma conta diferente daquela que criou inicialmente a pasta, como o administrador, o processo de mesclagem falhará.

Apêndice C. Ferramentas da Linha de Comandos

Os recursos do ThinkVantage Technologies também podem ser chamados localmente ou remotamente por administradores de TI corporativos por meio da interface da linha de comandos. As definições de configuração podem ser mantidas por meio de definições remotas de arquivo de texto.

Antidote Delivery Manager

Mailman

Utiliza o comando C:\Arquivos de programas\IBM ThinkVantage\Rescue and Recovery\ADM\mailman.exe. Esse programa verificará no Repositório do Antidote as tarefas a serem executadas. Não existem argumentos da linha de comandos.

Assistente do Antidote

Este comando, AWizard.exe está localizado onde quer que o administrador instalá-lo. Não existem argumentos da linha de comandos.

Configurar Senhas

Para uma discussão sobre senhas, consulte “Senhas” na página 34.

CFGMOD

O CFGMOD fornece um método de atualização do arquivo TVT.TXT por meio de um script. O comando CFGMOD encontra-se no diretório C:\Arquivos de programas\IBM ThinkVantage\Rescue and Recovery\ directory. Se você modificar o planejamento de backup, esse comando deverá ser seguido de RELOADSCHED. Esse utilitário deve ser executado com privilégios de administrador.

Sintaxe:

`cfgmod` *`TVT.TXT mod file`*

O formato do arquivo mod requer uma linha por entrada. Cada entrada inclui um número de seção (delimitado por [and]), seguido por um nome de parâmetro, seguido por "=", seguido pelo valor. Por exemplo, para ajustar o planejamento de backup, as entradas do arquivo mod deveriam ser as seguintes:

```
[rescuerecovery]ScheduleFrequency=1
[rescuerecovery]ScheduleHour=8
[rescuerecovery]ScheduleMinute=0
```

Client Security Solution

O Client Security Solution tem as seguintes ferramentas de linha de comandos:

SafeGuard PrivateDisk

A interface da linha de comandos está localizada na pasta C:\Arquivos de programas\IBM ThinkVantage\SafeGuard PrivateDisk\. A sintaxe é:

```
PDCMD
 [ADDCERT nome_volume /pw senha_admin /sn NS_cert [/acc access]]  |
 [LIST]  |
 [MOUNT nome_volume [/pw senha_usuário [/pt modo_aut]] [/ro]]  |
 [NEW nome_volume [/sz tamanho] [/dl letra_unidade] [/fs filesystem]
   [/pw senha_admin] [/pwu senha_usuário]]  |
 [UNMOUNT nome_volume /f]  |
 [UNMOUNTALL [/f]]  |
 [SETPASSWORD ome_volume /pw senha_admin /pwu senha_usuário [/ro]]
```

Os parâmetros são mostrados na Tabela 46:

Tabela 46.

Parâmetro	**Resultado**
ADDCDERT	Inclui um certificado no volume PrivateDisk.
LIST	Lista os volumes PrivateDisk deste usuário.
MOUNT	Monta um volume PrivateDisk específico.
NEW	Cria um novo volume PrivateDisk.
UNMOUNT	Desmonta um volume PrivateDisk específico.
UNMOUNTALL	Desmonta todos os volumes PrivateDisk.
SETPASSWORD	Configura a senha do usuário em um volume PrivateDisk.
volumename	O nome do arquivo que contém os arquivos PrivateDisk.
pw	A senha
sn	Número de série do certificado.
acc	Tipo de acesso do certificado a ser incluído. Os valores válidos são: • **adm** acesso de administrador • **uro** acesso de leitura de usuário • **usr** acesso de gravação de usuário (padrão)
pt	Método de autenticação. Os valores válidos são: • **0** Acesso de administrador (padrão) • **1** Senha de Usuário • **2** PIN para um login baseado em certificado
ro	Somente leitura.
sz	Tamanho (em Kbytes).
dl	Letra da unidade do volume PrivateDisk (padrão=próxima letra de unidade disponível).

Tabela 46. (continuação)

Parâmetro	Resultado
fs	O Sistema de Arquivos. Os valores padrão são: • FAT (padrão) • NTFS
pwu	Senha de Usuário
f	Forçar a operação

Security Advisor

Para executar esta ferramenta na GUI, clique em **Iniciar->Programas->ThinkVantage->Client Security Solution**. Clique em **Advanced** e escolhe **Audit Security Settings**. Isso executará C:\Arquivos de programas\IBM ThinkVantage\Common\WST\wst.exe para uma configuração padrão.

Os parâmetros são:

Tabela 47.

Parâmetros	Descrição
HardwarePasswords	Pode ser 1 ou 0: 1 mostrará esta seção, 0 a ocultará. Se não estiver presente, ela será mostrada por padrão.
PowerOnPassword	Configura o valor que uma senha de Ligação deve estar ativada, caso contrário a configuração será sinalizada.
HardDrivePassword	Configura o valor que uma senha de Disco Rígido deve estar ativada, caso contrário a configuração será sinalizada.
AdministratorPassword	Configura o valor que uma senha de Administrador deve estar ativada, caso contrário a configuração será sinalizada.
WindowsUsersPasswords	Pode ser 1 ou 0: 1 mostrará esta seção, 0 a ocultará. Se não estiver presente, ela será mostrada por padrão.
Password	Configura o valor que uma senha do usuário deve estar ativada, caso contrário a configuração será sinalizada.
PasswordAge	Configura o valor de qual deve ser a idade da senha do Windows nesta máquina para que a configuração não seja sinalizada.
PasswordNeverExpires	Configura o valor que a senha do Windows nunca pode expirar, caso contrário a configuração será sinalizada.
WindowsPasswordPolicy	Pode ser 1 ou 0: 1 mostrará esta seção, 0 a ocultará. Se não estiver presente, ela será mostrada por padrão.
MinimumPasswordLength	Configura o valor que o comprimento da senha deve ter nesta máquina para que a configuração não seja sinalizada.

Tabela 47. (continuação)

Parâmetros	Descrição
MaximumPasswordAge	Configura o valor que a idade da senha deve ter nesta máquina para que a configuração não seja sinalizada.
ScreenSaver	Pode ser 1 ou 0: 1 mostrará esta seção, 0 a ocultará. Se não estiver presente, ela será mostrada por padrão.
ScreenSaverPasswordSet	Configura o valor que a proteção de tela deve ter senha, caso contrário a configuração será sinalizada.
ScreenSaverTimeout	Configura o valor que o tempo limite do protetor de tela deve ter nesta máquina para que a configuração não seja sinalizada.
FileSharing	Pode ser 1 ou 0: 1 mostrará esta seção, 0 a ocultará. Se não estiver presente, ela será mostrada por padrão.
AuthorizedAccessOnly	Configura o valor que o acesso autorizado deve ser configurado para compartilhamento de arquivos, caso contrário a configuração será sinalizada.
ClientSecurity	Pode ser 1 ou 0: 1 mostrará esta seção, 0 a ocultará. Se não estiver presente, ela será mostrada por padrão.
EmbeddedSecurityChip	Configura o valor que o chip de segurança deve ser ativado, caso contrário a configuração será sinalizada.
ClientSecuritySolution	Configura o valor de qual deve ser a versão do CSS nesta máquina para que a configuração não seja sinalizada.

Outra opção para todos os valores é ignore, que significa mostrar o valor mas não incluir esse valor na comparação. Enquanto o Security Advisor estiver em execução um arquivo HTML será gravado em c:\ibmshare\wst.html e um arquivo XML de dados brutos será gravado em c:\ibmshare\wst.xml

Exemplo

Esta é uma Seção [WST] que mostra todas as seções e tem todas as configurações definidas como seus valores padrão:

```
[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 ou customizar o Security Advisor, inclua uma seção no arquivo TVT.txt com o nome WST. Existem vários valores que podem ser ocultados ou customizados, mas precisam ser incluídos no arquivo TVT.txt.

Se você não quiser utilizar o Security Advisor e não quiser que ele apareça ativado na GUI, remova o seguinte executável:

```
C:\Arquivos de programas\IBM ThinkVantage\Common\WST\wst.exe
```

Assistente de Transferência de Certificado

Se você não quiser utilizar o Assistente de Transferência de Certificado e não quiser que ele apareça ativado na GUI, remova o seguinte executável:

```
C:\Arquivos de programas\IBM ThinkVantage\Client Security Solution
\certificatetransferwizard.exe
```

Assistente do Client Security

Este Assistente é utilizado para assumir a Propriedade do hardware, configurar o software e inscrever usuários. Também é usado para gerar scripts de implementação por meio de arquivos XML. O comando a seguir pode ser executado para compreender as funções do assistente:

```
C:\Arquivos de programas\IBM ThinkVantage\Client Security Solution\css_wizard.exe /?
```

Tabela 48.

Parâmetro	**Resultado**
/h ou /?	Exibe a caixa da mensagem de ajuda
/name:*FILENAME*	Precede o caminho completo e o nome do arquivo de implementação gerado. O a terá uma extensão .xml.
/encrypt	Criptografa o arquivo de script utilizando criptografia AES. O nome do arquivo terá .enc anexado ser for criptografado. Se o comando /pass não for utilizado, uma passphrase estática será utilizada para obscurecer o arquivo.
/pass:	Precede a passphrase para proteção do arquivo de implementação criptografado.
/novalidate	Desativa os recursos de verificação de Senha e Passphrase do assistente para que um arquivo de script possa ser criado em uma máquina já configurada. Por exemplo, a senha do Administrador na máquina atual pode não ser a senha do Administrador desejada em toda a empresa. Utilize o comando /novalidate para poder digitar uma senha de Administrador diferente na GUI do css_wizard durante a criação do arquivo XML.

Eis um exemplo desse comando:

```
css_wizarde.exe /encrypt /pass:my secret /name:C:\DeployScript /novalidate
```

Nota: Se o sistema estiver executando no modo de emulação, o nome do executável será css_wizard.exe

Ferramenta de Criptografia/Decriptografia de Arquivo de Implementação

Essa ferramenta é utilizada para criptografar/decriptografar arquivos de implementação XML do Client Security. O comando a seguir pode ser executado para compreender as funções da ferramenta:

```
C:\Arquivos de programas\IBM ThinkVantage\Client Security Solution\
xml_crypt_tool.exe. /?
```

Os parâmetros são mostrados na Tabela 49:

Tabela 49.

Parâmetros	Resultados
/h ou /?	Exibe a mensagem de ajuda
FILENAME	O caminho completo e o nome do arquivo com a extensão .xml ou .enc
encrypt ou decrypt	Selecione /encrypt para arquivos .xml e /decrypt para arquivos .enc
PASSPHRASE	Um parâmetro opcional que é necessário se uma passphrase for utilizada para proteger o arquivo.

Exemplos:

```
xml_crypt_tool.exe "C:\DeployScript.xml" /encrypt "my secret"
```

e

```
xml_crypt_tool.exe "C:\DeployScript.xml.enc" /decrypt "my secret"
```

Ferramenta de Processamento de Arquivo de Implementação

A ferramenta vmserver.exe processa os scripts de implementação XML do Client Security. O comando a seguir pode ser executado para compreender as funções do assistente:

```
C:\Arquivos de programas\IBM ThinkVantage\Client Security Solution\vmserver.exe /?
```

Tabela 50.

Parâmetro	Resultado
FILENAME	O parâmetro FILENAME deve ter uma extensão de arquivo xml ou enc
PASSPHRASE	O parâmetro PASSPHRASE é utilizado para decriptografar um arquivo com a extensão enc

Eis um exemplo desse comando:

```
Vmservere.exe  C:\DeployScript.xml.enc "my secret"
```

Nota: Se o sistema estiver executando no modo de emulação, o nome do executável será vmserver.exe

TPMENABLE.EXE

O arquivo TPMENABLE.EXE é utilizado para ativar ou desativar o chip de segurança.

Tabela 51.

Parâmetro	Descrição
/enable ou /disable (Ativar ou desativar o chip de segurança)	Ativa ou desativa o chip de segurança.
/quiet	Oculta avisos da Senha do BIOS ou erros
sp:*password*	Senha de Administrador/Supervisor do BIOS; não utilize aspas delimitando a senha

Comando de Amostra:

```
tpmenable.exe /enable /quiet /sp:My BiosPW
```

eGatherer

O comando eGatherer pode ser localizado em C:\Arquivos de programas\IBM ThinkVantage\common\egatherer\egather2.exe.

O egathere2.exe cria uma saída EG2 com as informações coletadas. Também pode criar um arquivo de saída XML local que é armazenado na pasta home. Observe que o arquivo EG2 é um formato interno.

Dois arquivos XML serão criados, um para as informações do sistema e um para as informações demográficas. O nome do arquivo XML é criado combinando o fabricante, modelo-tipo e número de série. Por exemplo: IBM-2373Q1U-99MA4L7.XML, IBM-2373Q1U-99MA4L7.DEMOGRAPHICS.XML .

O a pode ser executado a partir de uma linha de comandos utilizando a seguinte sintaxe da linha de comandos:

egather2.exe [-help] [-batch] [-silent] [-nolimit] [-local] [-listprobes] [-probe probename *probename*]

- **-help**

  Mostrar uma mensagem de ajuda resumida.
- **-batch**

  Não mostrar o disclaimer.
- **-silent**

  Não mostrar nada durante a operação.
- **-nolimit**

  Coletar o registro de eventos inteiro. O padrão é as últimas 500 entradas.
- **-local**

  Criar um arquivo XML local.
- **-listprobes**

  Listar as probes disponíveis.
- **-probe**

Executar as probes especificadas.

MAPDRV

O comando MAPDRV chamará a interface com o usuário para mapear uma unidade de rede. O comando MAPDRV.EXE pode ser localizado no diretório C:\Arquivos de programas\IBM ThinkVantage\Common\MND. A interface com a unidade de rede de mapa suporta os seguintes parâmetros

Sintaxe:

```
mapdrv [switches]
```

A digitação do comando sem nenhum parâmetro ativa o aplicativo e as informações precisarão ser digitadas manualmente.

Os códigos de retorno para todos os parâmetros são:

- **0** = sucesso
- **> 0** = com falha

Tabela 52. Parâmetros de MAPDRV

Parâmetro	Resultado
/nodrive	Estabelece conexão de rede sem designar a letra da unidade para a conexão.
/pwd	A senha para este usuário neste compartilhamento.
/set	Configura o compartilhamento, o usuário e a senha utilizados pelo Backup and Restore. Os códigos de retorno são:
/s	Silencioso. Não avisa o usuário, independentemente de a conexão ser estabelecida ou não.
/timeout	Configura o valor de tempo limite.
/unc	O nome do compartilhamento no formato \\servidor\compartilhamento.
/user	O nome do usuário deste compartilhamento.

Quando o comando /SET for utilizado, a seção a seguir será incluída no arquivo TVT.TXT. Isso é mostrado no seguinte exemplo, no qual os parâmetros /UNC/USER e PWD são utilizados:

```
mapdrv /set /unc sharename /user username /pwd password
[mapdrv]
UNC=\\test\test
User=1EE22597AE4D
PWD=04E22197B34D95943ED5A169A0407C5C
```

Controle do Gerenciador de Inicialização do Rescue and Recovery (BMGR32)

A interface de linha de comandos da interface com o gerenciador de inicialização é BMGR32. Ela reside no diretório C:\Arquivos de programas\IBM ThinkVantage\Common\BMGR. A tabela a seguir apresenta os comutadores e seus resultados para BMGR32.

Tabela 53. Parâmetros de BMGR32

bmgr32	Resultado
/B0	Inicializar na partição 0 (com base na ordem da tabela de partições)
/B1	Inicializar na partição 1
/B2	Inicializar na partição 2
/B3	Inicializar na partição 3
/BS	Inicializar na Partição de Serviço
/BW	Inicializar na partição protegida do Rescue and Recovery
/BWIN	Pedido de reconfiguração para inicializar em WINPE. Isso deve ser chamado antes da inicialização.
/CFG*file*	Aplicar os parâmetros do arquivo de configuração. Consulte “Interface da Linha de Comandos RRCMD” na página 165 para obter detalhes sobre o arquivo de configuração.
/DS	Retornar o setor de dados do MBR (base 0).
/D*n*	Aplicar as alterações no disco n, em que n tem base 0 (padrão: (disco contendo a variável de ambiente ″SystemDrive″ ou ″C:\″ se ″SystemDrive″ não estiver definida).
/H0	Ocultar partição 0.
/H1	Ocultar partição 1.
/H2	Ocultar partição 2.
/H3	Ocultar partição 3.
/HS	Ocultar a Partição de Serviço.
/P12	Ocultar a Partição de Serviço configurando o tipo de partição como 12.
/INFO	Exibir informações da unidade de disco rígido (procura 8 setores livres).
/INFOP	Exibir informações da unidade de disco rígido (procura 16 setores livres).
/M0	O ambiente do Rescue and Recovery está localizado na Partição de Serviço.
/M1	O ambiente do Rescue and Recovery está localizado no diretório C:\PARTITION (inicialização dupla Windows e Windows PE).
/M2	O ambiente do Rescue and Recovery está localizado na Partição de Serviço com o DOS (inicialização dupla Windows PE e DOS; somente de marca Lenovo ou IBM pré-carregado).
/OEM	O computador não é um computador IBM ou Lenovo. Isso força uma segunda verificação da tecla F11 (padrão), pressionada após o POST. Isso pode ser necessário para sistemas IBM mais antigos. Essa também é a configuração padrão para a versão OEM do Rescue and Recovery.
/Patch *n*	Utilizado apenas para o programa de instalação para definir uma variável que um programa de correção MBR pode acessar.
Patchfile *filename*	Utilizado apenas para o programa de instalação instalar uma correção MBR

Tabela 53. Parâmetros de BMGR32 (continuação)

bmgr32	Resultado
/PRTC	Utilizado apenas para o programa de instalação recuperar o código de retorno da correção
/IBM	O sistema é um computador IBM ou Lenovo
/Q	silencioso
/V	prolixo
/R	Reinicializar computador
/REFRESH	Reconfigurar as entradas da tabela de partições no setor de dados
/TOC *tocvalue*	Configurar o local de TOC do BIOS (1 caracteres que representam 8 bytes de dados)
/U0	Mostrar partição 0
/U1	Mostrar partição 1
/U2	Mostrar partição 2
/U3	Mostrar partição 3
/US	Mostrar a partição de serviço
/F*mbr*	Carregar o programa de registro de inicialização principal RRE.
/U	Descarregar o programa de registro de inicialização principal RRE.
/UF	Forçar instalação ou desinstalação do programa MBR
/?	Listar as opções da linha de comandos.

Quando bmgr.exe é chamado com um atributo /info, as seguintes informações são descarregadas no dump:

- **MBR Adicional**

  Números dos setores que contêm o MBR, além do primeiro setor.
- **Dados**

  Número de setor do setor de dados utilizado pelo MBR.
- **Índices de correções**

  Números dos setores de quaisquer correções aplicadas utilizando o MBR.
- **Retorno do checksum**

  Deve ser 0 se não houve erros de checksum.
- **Partição de Inicialização**

  O índice com base 1 da Partição de Serviço na tabela de partições.
- **Partição Alt**.

  Índice da tabela de partições que aponta para a área inicializável do DOS, se existir
- **MBR Original**

  Número do setor onde o MBR original da máquina está armazenado.
- Sinalizador **IBM**

  Valor do setor de dados (1 se o sistema for IBM ou Lenovo, 0 em caso contrário)
- **Configuração de Inicialização**

Descreve a opção de instalação utilizada para descrever o layout da máquina. Se foi utilizada uma partição de serviço ou uma partição virtual.

- **Assinatura**

  Valor da assinatura localizado no setor de dados e no primeiro setor, deve conter "NP"

- **Duração da Pausa**

  Este é o número de ¼ de segundos a aguardar se a Mensagem de F11 for exibida na tela.

- **Código de Varredura**

  Qual tecla é utilizada ao inicializar para a Área de Serviço. 85 é para a tecla F11.

- **RR**

  Não utilizado pelo BMGR, é configurado pelo Rescue and Recovery.

- **Partição Ativa Anterior**

  Enquanto inicializado para a Área de Serviço, este valor contém o índice da tabela de partições da partição ativa anteriormente.

- **Estado de Inicialização**

  Utilizado pelo MBR para determinar o estado atual da Máquina. 0 – Inicializar normal para o S.O., 1 – Inicializar para o S.O. de Serviço, 2 – Inicializar de volta ao S.O. normal do S.O. de Serviço.

- **Sinalizador de Inicialização Alternativa**

  Inicializar para o S.O. alternativo, por exemplo, DOS

- **Tipo da Partição Anterior**

  Quando inicializado para a Área de Serviço, este valor contém o tipo de partição com que a Partição de Serviço foi configurada antes de inicializar para ela.

- **Índice MBR IBM Anterior**

  Usado pelo instalador.

- **Correção ENTRADA: SAÍDA**

  Valores de entrada e de saída do código de correção, se utilizado.

- **Msg de F11**

  Mensagem a ser exibida ao usuário se chamadas de BIOS corretas não forem suportadas.

RELOADSCHED

Este comando recarrega as configurações planejadas definidas no TVT.TXT. Se você fizer alterações no TVT.TXT para planejamento, deverá executar esse comando para ativar as alterações.

Comando de Amostra:

```
C:\Arquivos de programas\IBM ThinkVantage\Rescue and Recovery\reloadsched
```

Interface da Linha de Comandos RRCMD

A interface da linha de comandos primária do Rescue and Recovery é RRCMD. O comando está localizado no subdiretório C:\Arquivos de programas\IBM ThinkVantage\Rescue and Recovery\reloadsched.exe. Consulte as informações a seguir para utilizar a interface da linha de comandos do Rescue and Recovery.

Sintaxe:

```
RRcmd comando filter=filterfile location=c [name=abc | level=x] [silent]
```

Tabela 54. Parâmetros de RRCMD

Comando	Resultado
`Backup`	Iniciar uma operação normal de backup (deve incluir parâmetros de local e nome).
`Restore`	Iniciar uma operação normal de restauração (deve incluir local e nível).
`List`	Listar arquivos incluídos no nível de backup (deve incluir local e nível).
`Basebackup`	Iniciar um backup alternativo básico. Isso não deve ser utilizado como um fundamento para backups incrementais e deve incluir o local, o nome e o nível. O nível deve ter menos de 99. Se já existir outro backup básico com o mesmo nível, ele será sobrescrito.
`Sysprepbackup`	Preparar uma operação de backup na Área de Pré-Desktop depois que o computador for reinicializado. O principal uso desse recurso é capturar um backup Sysprep. **Notas:** 1. Em alguns casos, a barra de progresso não se movimentará. Se isso ocorrer, você poderá verificar se o backup está ocorrendo ouvindo a unidade de disco rígido. Quando o backup estiver concluído, você receberá uma mensagem indicando isso. 2. Se você estiver configurando uma senha ao criar um sysprepbackup na rede, o arquivo da senha não será gravado no local do backup até que seja executado um backup incremental. Eis duas soluções alternativas: a. Crie um backup sysprep local e copie os backups para a rede ou para o USB. b. Crie um backup incremental para a rede ou o USB após o backup sysprep e mantenha ou exclua o backup incremental.
`Copy`	Copiar backups de um local para outro. Isso também é conhecido como archive e deve incluir o local.
`Rejuvenate`	Renovar o sistema operacional para o backup especificado.
`Delete`	Excluir backups. Isso deve incluir o local.
`Changebase`	Alterar arquivos em todos os backups com base no conteúdo de file.txt. As opções em file.txt são: **A** Incluir **D** Excluir **RS** Substituir
`migrate`	Criar arquivo de migração a partir de um backup.
`filter=`*`filterfile`*	Identifica quais arquivos e pastas serão restaurados e não altera outros arquivos. Isso é utilizado apenas com o comando **restore**.

Tabela 54. Parâmetros de RRCMD (continuação)

Comando	Resultado
`Location=c`	Um ou mais dos seguintes pode ser selecionado com o resultado associado. **L** Para unidade de disco rígido local principal **U** Para unidade de disco rígido USB **S** Para segunda unidade de disco rígido local **N** Para rede **C** Para restauração por CD/DVD
`name=abc`	Em que *abc* é o nome do backup.
`level=x`	Em que *x* é um número de 0 (para o básico) até o número máximo de backups incrementais (utilizado apenas com a opção de restauração). Para comandos de backup, o comando level=*x* será necessário apenas se executar um backup de administrador (igual ou maior do que 100, por exemplo). **Notas:** 1. Para restaurar a partir do último backup, não forneça este parâmetro. 2. Todos os recursos de backup e restauração são roteados por meio do serviço para que a seqüência apropriada possa ser mantida, os callbacks sejam executados, por exemplo. O comando de backup é substituído pelas opções de linha de comandos).

Formato do Arquivo de Configuração do Gerenciador de Inicialização	O formato do arquivo de configuração do gerenciador de inicialização é compatível retroativamente com a versão anterior do gerenciador de inicialização. Qualquer comutador não mostrado a seguir não será suportado. O formato de arquivo é um arquivo de texto com cada entrada em uma linha separada.
	
	`<PROMPT1=esse é o texto que aparecerá no prompt F11>`
	`<KEY1=F11>`
	`<WAIT=40>`

System Migration Assistant

O módulo é um programa da linha de comandos compatível com o SMA4.2 antigo SMABAT.EXE. Os parâmetros do comando e o cartão de controle (Commands.TXT) para o módulo devem ser compatíveis com o SMA 4.2.

Active Update

Active Update é uma tecnologia eSupport que utiliza os clientes de atualização no sistema local para entregar os pacotes desejados na Web sem nenhuma interação com o usuário. O Active Update consulta os clientes de atualização disponíveis e utiliza o cliente de atualização disponível para instalar o pacote desejado. O Active Update ativará o ThinkVantage System Update ou o Instalador de Software no sistema.

Para determinar se o Ativador do Active Update está instalado, verifique a existência da seguinte chave de registro:
HKLM\Software\Thinkvantage\ActiveUpdate

Para determinar se o Ativador do Active Update está configurado para permitir o Active Update, o HKLM\Software\IBMThinkvantage\Rescue and Recovery deve verificar em sua própria chave de registro o valor do atributo EnableActiveUpdate. EnableActiveUpdate=1 configurará o item de menu Active Update no menu Ajuda.

Active Update

Para determinar se o Ativador do Active Update está instalado, verifique a existência da seguinte chave de registro:

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

Para determinar se o arquivo TVT.TXT está configurado para permitir o Active Update, o TVT deve verificar em sua própria chave de registro o valor do atributo EnableActiveUpdate. Se EnableActiveUpdate=1, o TVT deve incluir o item de menu Active Update no menu Ajuda.

Para chamar o Active Update, o TVT responsável pela chamada deve ativar o programa Ativador do Active Update e transmitir um arquivo de parâmetros (Consulte Arquivo de Parâmetros do Active Update para uma descrição do arquivo de parâmetros).

Utilize as seguintes etapas para chamar o Active Update:

1. Abra a chave de registro do Ativador do Active Update:

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

2. Obtenha o valor do atributo Path.
3. Obtenha o valor do atributo Program.
4. Concatene os valores encontrados nos atributos Path e Program para formar a cadeia do comando.
5. Anexe o arquivo de parâmetro (consulte Arquivo de Parâmetros do Active Update) à cadeia do comando.
6. Execute a cadeia do comando. Eis um exemplo de como poderá ser a cadeia de comando resultante:

   ```
   C:\Arquivos de programas\ThinkVantage\ActiveUpdate\activeupdate.exe
   C:\Arquivos de programas\ThinkVantage\RnR\tvtparms.xml
   ```

A maneira recomendada de chamar o Active Update é assincronamente para que o TVT responsável pela chamada não seja bloqueado. Se o TVT responsável pela chamada precisar ser encerrado antes de instalar a atualização, é responsabilidade do programa de instalação da atualização encerrar o TVT.

Arquivo de Parâmetros do Active Update

O arquivo de parâmetros do Active Update contém as configurações a serem transmitidas para o Active Update. Atualmente, somente TargetApp (o nome do TVT) é transmitido, conforme mostrado neste exemplo:

```
<root>
       <TargetApp>ACCESSIBM</TargetApp>
</root>
<root>
       <TargetApp>1EA5A8D5-7E33-11D2-B802-00104B21678D</TargetApp>
</root>
```

Apêndice D. Ferramentas do Administrador

As tecnologias ThinkVantage oferecem ferramentas que podem ser chamadas por administradores de TI corporativos.

Assistente do Antidote

Para informações sobre o assistente do Antidote, consulte o Apêndice F, "Referência e Exemplos de Comandos do Antidote Delivery Manager", na página 175.

BMGR CLEAN

CleanMBR limpa o MBR (Registro de Inicialização Master). Este programa pode ser utilizado quando você encontrar uma falha de instalação do Rescue and Recovery, tal como não conseguir instalar o Rescue and Recovery com um número menor que o necessário de setores livres para a instalação do gerenciador de inicialização.

Notas:

1. Depois de executar esta ferramenta, os aplicativos que estiverem utilizando o MBR serão inúteis. Por exemplo, o SafeGuard Easy, SafeBoot, a versão MBR do Computrace etc.
2. A ferramenta deve ser executada antes de instalar o Rescue and Recovery.
3. Utilize cleanmbr.exe para DOS e CleanMBR32.exe para Windows.
4. Depois de executar CleanMBR no DOS, execute FDISK /MBR; isso colocará o MBR.

Os parâmetros para CleanMBR32.exe são:

Tabela 55.

Parâmetro (Exigido):	**Descrição**
/A	Limpar o MBR e instalar o MBR do PC DOS.
Parâmetro (Opcional):	
/Dn	Aplicar alterações na unidade. Utilize *n*=0 para a primeira unidade.
/Y	Sim para tudo.
/?	Exibir a Ajuda.
/H	Exibir a Ajuda.

CLEANDRV.EXE

Limpa todos os arquivos da unidade. Não existirá um sistema operacional após a execução deste comando. Consulte "Instalando o Rescue and Recovery em uma Partição de Serviço do Tipo 12" na página 126 para obter informações adicionais.

CONVDATE

O utilitário Convdate é fornecido como parte das ferramentas de Administração do Rescue and Recovery. Este utilitário é utilizado para determinar os valores HEX de data e hora e para converter valores de data e hora em valores HEX, e pode ser utilizado para configurar uma data e hora customizada em um campo de backup de TVT.TXT

```
[Backup0]
StartTimeLow=0xD5D53A20
StartTimeHigh=0x01C51F46
```

Para executar o utilitário, faça o seguinte:

1. Extraia as ferramentas de Administração do Rescue and Recovery de http://www.lenovo.com/thinkvantage.
2. Abra uma janela de comandos.
3. Digite Convdate.

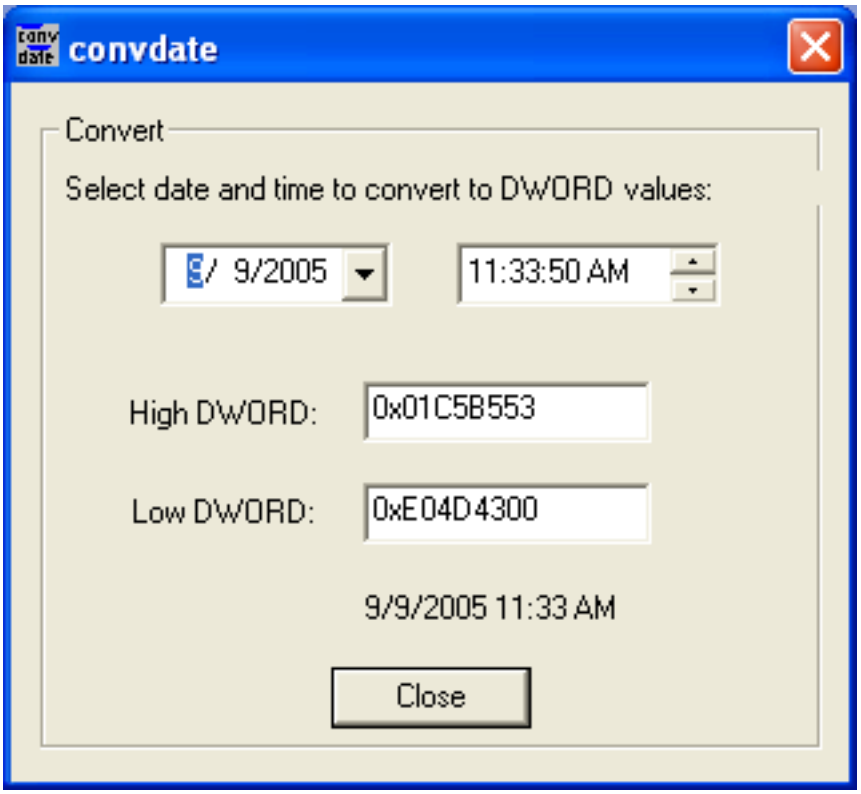

Figura 5. Janela de Convdate

4. Digite a Data e Hora nos campos sob Select date and time to convert DWORD Values.
5. Os valores correspondentes no arquivo TVT..TXT file são:
   - High DWORD=StartTimeHigh
   - Low Dword=StartTimeLow

CREAT SP

Este comando cria uma partição para a Partição de Serviço com os megabytes desejados. A letra da unidade é opcional.

A sintaxe é:

```
createsp size=x drive=x /y
```

Os parâmetros para CREAT SP são:

Tabela 56.

Parâmetros	Descrição
size=*x*	Tamanho da partição de serviço a ser criada, em Megabytes.
drive=*x*	O número da unidade na qual a partição de serviço deve ser criada. Se não for especificado, será utilizada a primeira unidade não USB. Este parâmetro é opcional.
/y	Suprime a confirmação da unidade que está sendo limpa. Este parâmetro é opcional.

Nota: bmgr32.exe deve estar no mesmo diretório que createsp.exe, e deve ser executado no WinPE.

RRUTIL.EXE

Para obter informações sobre RRUTIL.EXE, consulte “Área Pré-desktop” na página 19.

SP.PQI

Este arquivo pode ser utilizado para criar uma partição de serviço Tipo 12. Consulte “Instalando o Rescue and Recovery em uma Partição de Serviço do Tipo 12” na página 126 para obter informações adicionais.

Apêndice E. Tarefas do Usuário

Talvez os usuários não possam executar determinadas tarefas, dependendo dos direitos do usuário. As tabelas a seguir resumem os recursos das tarefas básicas com as permissões padrão para o ID de usuário do S.O. para o Usuário Limitado/Usuário, Usuário Avançado e Administrador. As tarefas e os recursos diferem por sistema operacional do Windows.

Windows XP

A tabela a seguir apresenta as tarefas que os usuários Limitados, Avançados e Administrativos podem executar no Rescue and Recovery em um ambiente Windows XP.

Tabela 57. Tarefas do Usuário do Windows XP

Os Usuários do Windows XP Podem Executar o Seguinte:	**Usuário Limitado**	**Usuário Avançado**	**Administrador**
Criar ISO de mídia de resgate	Não	Não	Sim (com linha de comandos fornecida abaixo)
Criar mídia de CD inicializável	Sim	Sim	Sim
Criar mídia inicializável de unidade de disco rígido USB	Não	Não	Sim
Iniciar backup	Sim	Sim	Sim
Inicializar restauração no RRE (Rescue and Recovery Environment)	Sim	Sim	Sim
Executar restauração de arquivo simples no RRE	Não (Windows) Sim (Área de Pré-inicialização do Windows)	Não (Windows) Sim (Área de Pré-inicialização do Windows)	Sim
Definir include e exclude na interface do Rescue and Recovery	Sim	Sim	Sim
Fazer backup em uma unidade de rede	Sim	Sim	Sim
Planejar backups	Sim	Sim	Sim

Windows 2000

A tabela a seguir apresenta as tarefas que os usuários Limitados, Avançados e Administrativos podem executar no Rescue and Recovery em um ambiente Windows 2000.

Tabela 58. Tarefas do Usuário do Windows 2000

Os Usuários do Windows 2000 Podem Executar o Seguinte:	**Usuário Limitado**	**Usuário Avançado**	**Administrador**
Criar ISO de mídia de resgate	Não	Não	Sim (com linha de comandos fornecida abaixo)

Tabela 58. Tarefas do Usuário do Windows 2000 (continuação)

Os Usuários do Windows 2000 Podem Executar o Seguinte:	Usuário Limitado	Usuário Avançado	Administrador
Criar mídia de CD inicializável	Sim	Sim	Sim
Criar mídia inicializável de unidade de disco rígido USB	Não	Não	Sim
Iniciar backup	Sim	Sim	Sim
Inicializar restauração no RRE (Rescue and Recovery Environment)	Sim	Sim	Sim
Executar restauração de arquivo simples no RRE	Não (Windows) Sim (Área de Pré-inicialização do Windows)	Não	Sim
Definir include e exclude na interface do Rescue and Recovery	Sim	Sim	Sim
Fazer backup em uma unidade de rede	Não	Não	Sim
Planejar backups	Sim	Sim	Sim

Criar Mídia de Resgate

Os administradores podem utilizar as seguintes linhas de comandos para criar o ISO de Mídia de Resgate. Essas linhas de comandos permitirão a criação do arquivo ISO necessário e ele será colocado automaticamente no diretório C:\Arquivos de programas\IBM ThinkVantage\Rescue and Recovery\rrcd\.

```
:: This line will create the ISO silently and not burn it

C:\Arquivos de programas\IBM ThinkVantage\Common\Python24\python"
"C:\Arquivos de programas\IBM ThinkVantage\Common\spi\mkspiim.pyc /scripted


 /scripted

:: This line will create the ISO with user interaction and not burn it

C:\Arquivos de programas\IBM ThinkVantage\Common\Python24\python
C:\Arquivos de programas\IBM ThinkVantage\Common\spi\mkspiim.pyc /noburn

 /noburn
```

Apêndice F. Referência e Exemplos de Comandos do Antidote Delivery Manager

Uma ferramenta de compactação de linha de comandos é fornecida para o administrador criar mensagens. Além disso, o Antidote Delivery Manager fornece algumas funções de comandos especiais para serem utilizadas nas mensagens.

Guia de Comandos do Antidote Delivery Manager

A interface de linha de comandos da interface com o gerenciador de inicialização é BMGR32. Ela reside no diretório C:\Arquivos de programas\IBM ThinkVantage\Rescue and Recovery\ADM. A tabela a seguir apresenta os comutadores e seus resultados para BMGR32.

Tabela 59. Comandos do Antidote Delivery Manager

Comandos	Descrição
APKGMES [/KEY *keyfile*|/NEWKEY *keyfile*|/NOSIG] *diretório_da_mensagem nome_da_mensagem*	Para APKGMES /KEY, um arquivo de mensagem será criado a partir do conteúdo de *TVT.TXT diretório_da_mensagem*. O diretório deve conter um arquivo denominado GO.RRS. Se o parâmetro /KEY for utilizado, uma chave de conexão será recuperada do keyfile.prv e a chave keyfile.pub deverá ter sido distribuída a todos os clientes que processarão a mensagem. Por padrão, o arquivo de chave "KEYFILE.PRV" será utilizado. O parâmetro /NEWKEY pode ser utilizado para criar uma chave. Se não desejar um sinal, especificar /NOSIG evitará o sinal. Uma date stamp será anexada ao final do nome da mensagem, como *nome_da_mensagem*YYMMDDHHmm.zap.
REBOOT [/*RR*|/Win] [/wait | /f]	Este comando reinicializa a máquina. Sem parâmetros, reinicialize com a seqüência normal de inicialização. O parâmetro RR significa reinicializar no Rescue and Recovery e WIN significa reinicializar no sistema operacional normal. A reinicialização não ocorrerá até a saída do script, de modo que esse deve ser normalmente o último comando de um script. O comando WAIT opcional força o sistema a inicializar no ambiente especificado na próxima reinicialização (manual ou causada por outro mecanismo). O parâmetro /f força o sistema a reinicializar agora e não permite que o usuário salve informações de aplicativos abertos. Se nenhum parâmetro for especificado, o programa utilizará o padrão /win (/wait e /f não são especificados).
RETRYONERROR [ON|OFF] *retries*	Por padrão, um script será tentado apenas uma vez. Entretanto, se for importante continuar a tentar um script até que ele funcione, o comando RETRYONERROR poderá ser utilizado para notificar a função de caixa postal para continuar a tentar executar esse script um número finito de vezes, conforme especificado pelo parâmetro retries. Se nenhum número for especificado, o valor padrão será 3. Um valor padrão global poderá ser definido no arquivo TVT.TXT, na seção de resgate `retries = retries`. Retries poderá ser definido também como FOREVER que causaria um loop infinito.

Tabela 59. Comandos do Antidote Delivery Manager (continuação)

Comandos	Descrição
`MSGBOX /msg texto_da_mensagem [/head texto_do_cabeçalho] [/OK] [/CANCEL]| [/TIMER tempo_limite] /B3`	O comando MSGBOX exibirá uma mensagem ao usuário final, se ele tiver efetuado logon. A mensagem permanecerá exibida e o script ficará bloqueado até o tempo limite ter decorrido, o botão de cancelamento ser pressionado ou o botão **OK** ser pressionado (se /OK estiver especificado). Um botão de cancelamento não será exibido no painel se /CANCEL não estiver especificado e não será fácil livrar-se da exibição. O comando retornará: • 0 = OK foi pressionado • 1 = CANCELAR • 2 = Cronômetro expirado O texto na mensagem pode ser formatado utilizando \n e \t para representar uma nova linha e uma guia, respectivamente.
`NETWK [/D|/E|/A [/IP endereço_ip | /DN nome_do_domínio] [/NM netmask]`	NETWK /D (desativar) interromperá todo o tráfego na rede, desativando todos os adaptadores de rede. A rede ficará desativada até que um comando NETWK /E (ativar) seja executado. NETWK /A restringe a rede ao endereço IP especificado pelo comutador /IP (decimal com pontos) ou /DN (nome do DNS). O comutador /NM fornece a máscara de rede. Se /NM não for fornecido, então apenas a máquina simples especificada pelo /IP ou /DN estará acessível. O estado desse comando persiste sobre as reinicializações, de modo que a rede deverá estar explicitamente ativada.
`APUBKEY [/ADD|/DELETE] chave_pública_codif_asn_1`	O comando APASSWD permite que um administrador gerencie remotamente as teclas de sinal da mensagem do Antidote Delivery Manager em cada PC. Mais de uma tecla pode ser armazenada em cada PC. Se uma mensagem assinada for processada, todas as chaves serão tentadas até que uma bem-sucedida seja encontrada. As chaves não são nomeadas separadamente, portanto devem ser referidas pelo conteúdo. Uma nova chave pode ser incluída com o parâmetro ADD e excluída com o parâmetro DELETE. Lembre-se de que se houver alguma chave especificada no TVT.TXT, as mensagens não assinadas (aquelas construídas com /NOSIG) não poderão mais ser utilizadas.
`AUNCPW [/Add|/CHANGE|/DELETE] unc [/USER userid] [/PWD senha] [/REF nome_de_ref]`	Este comando permite incluir, alterar ou excluir uma senha de uma unidade de rede. O nome de referência pode ser utilizado como atalho em uma mensagem, em vez de utilizar o UNC. Os valores de retorno são: • 0 = bem-sucedido • 1 = impossível definir com as informações fornecidas • 2 = bem-sucedido, mas um UNC diferente com o mesmo nome de referência já foi definido.

Tabela 59. Comandos do Antidote Delivery Manager (continuação)

Comandos	Descrição
`XMLtool for Conditionals`	Condicionais (eGatherer, informações atuais sobre o hardware) • **Uso:** xmltool.exe *nome_do_arquivo xpath função comparador valor* em que: – **nome_do_arquivo** O caminho e o nome do arquivo XML. – **xpath** O caminho de x completo para o valor. – **função** Deve ter um dos seguintes valores: - /C, comparar os valores (o comparador e o valor também devem ser fornecidos). - /F , colocar o valor especificado no %IBMSHARE%\RET.TXT. – **Comparador:** Deve ser um dos seguintes: - LSS - LEQ - EQU - GTR - GEQ - NEW – **Valor:** A entrada de XML é comparada a este valor. • Valores de Retorno: – **0** A comparação é avaliada como verdadeira (/c). – **1** A comparação é avaliada como falsa. – **2** Parâmetros de linha de comandos incorretos. – **3** Erro ao abrir o arquivo XML (não presente ou o arquivo contém erros). – **4** XPATH especificado não retornou um valor. • **Por exemplo:** `xmltool.exe %ibmshare%\\ibmegath.xml //resumo_do_sistema/versão_da_bios GEQ 1UET36WW.`
`INRR`	O comando INRR pode ser utilizado para determinar se o script está sendo executado no ambiente do Rescue and Recovery. Os valores de retorno são: • 0 = S.O. atual é o PE • 1 = O S.O. atual não é o PE • >1 = Erro

Tabela 59. Comandos do Antidote Delivery Manager (continuação)

Comandos	Descrição
`STATUS [/QUERY local nome_mens | /CLEAR local]`	O comando STATUS /QUERY pode ser utilizado para determinar se um script foi executado ou está na fila para ser executado. O valor de local deve ser um dos seguintes: • **FAIL** A mensagem já foi executada e falhou. • **SUCCESS** A mensagem foi concluída com êxito. • **WORK** A mensagem está sendo executada no momento ou será executada na próxima vez em que o Antidote Delivery Manager for executado. • **CACHE** A mensagem está na fila para ser executada. O comando STATUS/CLEAR limpará o *local* especificado. Os valores de retorno são: • 0 = se a mensagem especificada for localizada ou o comando for concluído com êxito. • 1 = se a mensagem especificada não for localizada ou o comando falhar.

Comandos da Microsoft Suportados

Tabela 60. Comandos Microsoft Suportados

Comandos	Descrição
`ATTRIB.EXE`	Exibe ou altera os atributos de arquivo.
`CACLS.EXE`	Exibe ou modifica as ACLs (Listas de Controle de Acesso) de arquivos.
`CHKDSK.EXE`	Verifica um disco e exibe um relatório de status.
`COMP.EXE`	Compara o conteúdo de dois arquivos ou conjuntos de arquivos.
`COMPACT.EXE`	Exibe ou altera a compactação de arquivos nas partições NTFS.
`CONVERT.EXE`	Converte volumes FAT em NTFS. Não é possível converter a unidade atual.
`DISKPART.EXE`	Particiona uma unidade.
`FC.EXE`	Compara dois arquivos ou conjuntos de arquivos e exibe as diferenças entre eles.
`FIND.EXE`	Procura uma cadeia de texto em um arquivo ou em arquivos.
`FINDSTR.EXE`	Procura cadeias em arquivos.
`FORMAT.COM`	Formata um disco para ser utilizado com Windows.
`LABEL.EXE`	Cria alterações ou exclui a etiqueta de volume de um disco.
`NET.EXE`	Fornece os comandos de rede.
`PING.EXE`	Verifica se um recurso de rede pode ser alcançado.

Tabela 60. Comandos Microsoft Suportados (continuação)

Comandos	Descrição
RECOVER.EXE	Recupera informações legíveis de um disco inválido ou com defeito.
REG.EXE	Manipulação de registros.
REPLACE.EXE	Substitui arquivo.
RRCMD.EXE	Executa Backups do S.O. ou restaura da entrada do S.O. ou de Classificações RR.
SORT.EXE	Classifica entrada.
SUBST.EXE	Associa um caminho a uma letra de unidade.
XCOPY.EXE	Copia árvores de arquivos e de diretórios.

Preparação e Instalação

Preparação

Se uma chave de conexão for utilizada, o administrador precisará executar a ferramenta de compactação com o parâmetro /NEWKEY para gerar uma nova chave de conexão.

Configuração

Vários itens de configuração serão necessários. Os itens aparecem no arquivo TVT.TXT:

Repositório

Todo cliente necessita de uma lista de repositórios. Isso pode incluir disquete e C:\, bem como pelo menos uma unidade de rede especificada com um UNC; `mailbox =` que é a unidade e o caminho para os locais de caixas postais, com uma vírgula e separados por ordem de importância. Por exemplo:

```
[rescue] mailbox = %y%\antidote, c:\antidote
```

Informações sobre o Planejamento

O Modo de Planejamento é a freqüência das verificações.

Tabela 61. Modos de Planejamento

Modo de Planejamento	
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

```
[Scheduler]
Task1=rescuerecovery
Task2=Rescue

[rescue]
ScheduleFrequency=0
ScheduleMode=0x02
TaskShow=1
Task=c:\Arquivos de programas\IBM ThinkVantage\Rescue and Recovery\adm\mailman.exe
ScheduleHour=11
ScheduleMinute=28
ScheduleDayOfTheWeek=3
ScheduleWakeForBackup=0
```

Chave de Conexão

Se chaves de sinal forem utilizadas, elas deverão ser distribuídas ao cliente. O arquivo keyfile.pub, criado pelo comando APKGMES, contém a chave. Toda chave de sinal pública autorizada aparece no arquivo TVT.TXT como: `pubkey`*X* `= ...` em que *X* é substituído por um inteiro e até 9 chaves públicas podem ser armazenadas. Utilize a função APUBKEY para definir esse valor `nosig =`. Se estiver definido como 1, permitirá que pacotes não assinados (pacotes construídos com o parâmetro /NOSIG) sejam executados.

Nota: Se não estiver definido como 1 ou se chaves públicas estiverem presentes no arquivo TVT.TXT, pacotes não assinados não serão executados.

Unidades de Rede

Os seguintes valores são definidos com a função AUNCPW `RscDrvY`. Toda seção `RscDrv` contém informações sobre um compartilhamento de rede. Até 10 compartilhamentos de rede podem ser definidos para o Antidote Delivery Manager.

- UNC = O UNC de uma unidade precisa que o Antidote Delivery Manager esteja conectado.
- User = Nome do usuário criptografado.
- Pwd = Senha criptografada.
- Ref = O nome de referência a ser associado a essa conexão.

Instalação em Clientes

O Rescue and Recovery 2.0 deve ser instalado em todos os clientes. A configuração preparada acima pode ser incluída na instalação ou executada posteriormente.

Infra-estrutura do Servidor

O administrador deve estabelecer compartilhamentos de rede para o repositório ou fornecer um site de FTP ou de HTTP. Um repositório adicional pode ser necessário para correções.

Teste de Sistema Simples – Notificação de Exibição

Preparo e Compactação de Script

Gravar um script GO.RRS em qualquer máquina em que o Antidote Delivery Manager esteja instalado. Inclua uma linha `MSGBOX /MSG "Hello World" /OK`. Execute o comando diretamente no prompt de comandos para assegurar que ele funciona da maneira desejada. Em seguida, execute o comando APKGMSG no

diretório que contém GO.RRS para criar uma mensagem. Coloque o arquivo de mensagens em um dos diretórios do repositório em sua máquina e observe se a operação está correta.

Implementação

Antes de implementar o Antidote Delivery Manager, execute estas etapas:

1. Determine os locais das caixas postais:
   - As *caixas postais* são definidas como diretórios em compartilhamentos de rede, em uma unidade de disco rígido ou em mídia removível em um sistema local, ou em um site FTP ou HTTP.
   - Pode ser útil ter várias caixas postais para o caso de uma delas não estar acessível. É possível definir até dez locais de caixas postais.
   - As caixas postais na rede devem ser de leitura para clientes e o acesso de gravação deve ser restrito.
2. Configure as caixas postais no arquivo TXT.TXT:
   - Em um sistema doador com o Rescue and Recovery instalado, edite o arquivo TVT.TXT localizado no diretório *C:\Arquivos de programas\IBM\ThinkVantage*.
   - Crie uma nova seção `rescue` no arquivo TVT.TXT.
   - Inclua a seguinte entrada na seção rescue:

     ```
     mailbox=
     ```

     e, em seguida, inclua as informações de diretório de sua caixa postal. As caixas postais na unidade local, por exemplo, seriam semelhantes a esta:

     ```
     [rescue]
     mailbox=C:\ADM\Mailbox,
      \\Network\Share
     ```

     As caixas postais em um site FTP seriam semelhantes a esta:

     ```
     ftp://ftp.yourmailbox.com
     ```

     As caixas postais em uma unidade de rede compartilhada seriam semelhantes a esta:

     ```
     \\Network\Share
     ```

     Notas:

     a. O HTTPS não é suportado para funções de caixa postal.

     b. O servidor Web HTTP deve estar configurado com fornecer indexação ativado e com o recurso de listar arquivos.

     As letras das unidades podem ser diferentes entre o Windows Professional Edition e seu ambiente normal de sistema operacional. A unidade C: é a mais provável de mudar. Para contornar isso, utilize a variável de ambiente *CUSTOS*, a qual sempre aponta para a unidade que contém o sistema operacional típico do cliente. O exemplo anterior seria alterado para:

     ```
     mailbox=%CUSTOS%\ADM\Mailbox,ftp://ftp.yourmailbox.com, \\Network\Share
     ```

     A cadeia pode ter qualquer comprimento, desde que respeita os padrões do dispositivo ou protocolo que está sendo utilizado. Por exemplo, se for utilizado um arquivo local, o caminho não pode exceder 256 caracteres.
   - Várias entradas de caixa postal são separadas por vírgulas ou ponto-e-vírgulas.

- O Antidote Delivery Manager procura pacotes seqüencialmente nos locais de caixas postais especificados.

3. Se for necessário um nome de usuário e uma senha para uma conexão FTP ou HTTP, utilize este formato:

   ```
   ftp//nome_do_usuário:senha@ftp.yourmailbox.com
   ```

4. Para caixas postais de compartilhamentos de rede com nome de usuário e senha:

   As entradas de nome do usuário e senha são armazenadas criptografadas no arquivo TVT.TXT. Para incluir uma entrada no sistema doador:

   a. Abra uma janela do DOS
   b. Mude para o diretório `C:\Arquivos de programas\IBM ThinkVantage\Rescue and Recovery\ADM`
   c. Execute este comando:

      ```
      auncpw /add \\Network\Share /user nome_do_usuário /pwd senha /ref refID
      ```

      Esse comando cria a seguinte entrada no arquivo TVT.TXT:

      ```
      [RscDrv0]
      UNC=\\Network\Share
      User=01E23397A54D949427D5AF69BF407D5C
      Pwd=04E22197B34D95943ED5A169A0407C5C
      Ref=refID
      ```

   Notas:

   a. Essa entrada pode ser usada em qualquer sistema a ser utilizado pelo Antidote Delivery Manager para obter acesso ao mesmo compartilhamento.
   b. Até 10 compartilhamentos de rede podem ser utilizados pelo Antidote Delivery Manager.
   c. Além dos 10 compartilhamentos de rede, outras entradas de caixas postais podem ser incluídas, como FTP ou locais.
   d. O arquivo AUNCPW.EXE tem outras funções que podem ser utilizadas para gerenciamento de senhas. Digite AUNCPW /? na linha de comandos ou consulte a Tabela 59 na página 175.

5. Crie o par de chaves Pública/Privada do Antidote Delivery Manager. Recomenda-se utilizar os recursos de par de chaves Pública/Privada do Antidote Delivery Manager. O Antidote Delivery Manager utiliza um par de chaves Pública/Privada para verificar a autenticidade de pacotes. A chave Privada deve ser guardada com cuidado e não deve ser distribuída. A chave Pública correspondente deve estar em todos os clientes gerenciados por meio do Antidote Delivery Manager. Para criar um par de chaves Pública/Privada em um sistema não doador com o Rescue and Recovery instalado:

   a. Abra uma janela do DOS.
   b. Emita um comando CD para C:\Arquivos de programas\IBM ThinkVantage\Rescue and Recovery\ADM.
   c. Execute este comando:

      ```
      apkgmes.exe /newkey mykey
      ```

      Esse comando cria dois arquivo, mykey.pub e mykey.prv; as chaves pública e privada, respectivamente.
   d. Copie a chave pública para o diretório C:\Arquivos de programas\IBM ThinkVantage\Rescue and Recovery\ADM do sistema doador.
   e. Abra o arquivo utilizando um programa editor de texto como o notepad.exe.
   f. Copie o conteúdo do arquivo para a área de transferência.

g. Na linha de comandos, digite o seguinte:

```
apubkey.exe /add x
```

em que *x* é o conteúdo da área de transferência.

h. Isso criará uma entrada no arquivo TVT.TXT na seção [rescue]: `pubkey0=906253...`.

- Até 10 chaves públicas podem ser armazenadas em TVT.TXT.
- O arquivo APUBKEY.EXE tem outras funções que podem ser utilizadas para gerenciamento de chaves Públicas. Na linha de comandos, digite `APUBKEY /?` ou consulte a Tabela 59 na página 175.

6. Crie a verificação de Planejamento do Antidote Delivery Manager (vários planejamentos são permitidos) que Antidote Delivery Manager precisa executar periodicamente no sistema. Para configurar um planejamento para ser executado a cada 20 minutos, inclua o seguinte no arquivo TVT.TXT no sistema doador:

```
[Scheduler]
Task1=rescuerecovery
Task2=egatherer
Task3=rescue

[rescue]
ScheduleFrequency=0
ScheduleMode=0x01
NumMinutes=20
TaskShow=1
Task=C:\Arquivos de programas\IBM ThinkVantage\Rescue and Recovery\ADM\antidote
\mailman.exe
```

em que *ScheduleMode* é o evento que acionará a entrega do pacote do Antidote Delivery Manager. Os parâmetros são:

Tabela 62. Parâmetros do Antidote Delivery Manager

Parâmetro	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. O planejador não executa na Área de Pré-Desktop.

b. Para obter informações adicionais, consulte "Planejando Backups e Tarefas Associadas" na página 151.

7. Crie um pacote do Antidote Delivery Manager.

Depois de concluir as etapas anteriores, construa e distribua seu primeiro pacote. Em um sistema Administrador (não doador), execute as seguintes etapas:

a. Crie um diretório como *C:\ADM\Build*.

b. Nesse diretório, crie um arquivo denominado GO.RRS e inclua o seguinte:

```
msgbox.exe /msg "Hello World!" /head "test" /ok /cancel
```

c. Salve e feche o arquivo.

d. Emita um comando CD para C:\Arquivos de programas\IBM ThinkVantage\Rescue and Recovery\ADM

e. Execute este comando:

```
apkgmes.exe /key mykey.prv C:\adm\build HELLOPKG
```

f. Isso criará um pacote denominado HELLOPKGYY*MMDDHHMM*.ZAP em que *AAMMDDHHMM* será substituído pela data/hora atual.

8. Copie HELLOPKGYY*MMDDHHMM*.ZAP para um local de caixa postal especificado na etapa 2.
9. Chame o Antidote Delivery Manager.
   a. Quando o cronômetro tiver expirado no sistema doador, o pacote será executado e uma caixa de mensagem Hello World aparecerá.
   b. Se você preferir não aguardar, poderá digitar no sistema doador: C:\Arquivos de programas\IBM ThinkVantage\Rescue and Recovery\ADM\mailman.exe

Exemplos

Os exemplos a seguir mostram algumas maneiras como o Antidote Delivery Manager pode ser utilizado:

Exemplo 1

Este exemplo é um pacote para corrigir um computador que constantemente exibe uma tela azul devido a um vírus ou a uma entrada incorreta no registro.

1. Suponha que o motivo pelo qual o computador cliente está exibindo uma tela azul é um vírus que é executado através da chave Run no registro. Para corrigir isso, é preciso criar um arquivo denominado go.rrs que execute *reg*. Consulte “Comandos da Microsoft Suportados” na página 178 para obter uma lista dos comandos da Microsoft. Reg remove o valor do registro e exclui o executável do sistema, se possível. O conteúdo deve ser semelhante a este:

   ```
   reg delete HKLM\Software\Microsoft\Windows\Current Version\Run /v runvirusvalue
   /f del %custos%\windows\system32\virus.exe
   ```

2. Agora, coloque o arquivo go.rrs no diretório *c:\adm\build* e execute:

   ```
   apkgmes.exe /key mykey.prv C:\adm\build REMOVEVIRUS
   ```

3. Copie REMOVEVIRUS*AADDHHMM*.ZAP para sua caixa postal.
4. Inicialize todos os clientes e pressione o botão Access IBM/F11 ou a tecla Enter para entrar na Área de Pré-Desktop na qual o arquivo mailman.exe será executado na inicialização e, em seguida, execute o pacote REMOVEVIRUS.

Exemplo 2

Este exemplo envia uma atualização ou correção do Quick Fix Engineering para as máquinas clientes.

1. Crie um diretório para conter o arquivo de script e os arquivos de correção, como *C:\adm\patchbuild*.
2. Coloque o qfe ou o executável de correção no diretório c:\adm\patchbuild.
3. Crie um arquivo denominado go.rrs e coloque nele as seguintes linhas, mas customize a linha que irá executar e instalar o Microsoft Quick Fix Engineering ou a correção. Como essa correção só pode ser instalada em um sistema operacional Windows regular, este script impede a instalação de tentar executar no Windows Professional Edition.

```
set custos
if errorlevel 1 set custos=%systemDrive%
%custos%\Arquivos de programas\IBM ThinkVantage\Rescue and Recovery\ADM
\retryonerror/on 10
%custos%\Arquivos de programas\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 ATIVAR A REDE
Netwk.exe /e
msgbox.exe /msg "Correção Instalada" /head "Concluído" /ok
exit 0

:InPE
exit 1
```

4. Coloque go.rrs no diretório c:\adm\patchbuild e execute:

   ```
   apkgmes.exe /key mykey.prv C:\adm\patchbuild PATCHBUILD
   ```

5. Copie PATCHBUILD*AADDHHMM*.ZAP para sua caixa postal.
6. A correção será instalada na próxima execução planejada do arquivo mailman.exe para a máquina cliente ou na reinicialização da máquina cliente.

Formas de Verificar se um Pacote Está Concluído ou Não

- **Registro de falhas**

  Este arquivo tipicamente é armazenado no diretório *c:\ibmtools\utils\rescue*. Se existir um arquivo zap com qualquer valor diferente de zero, ele será registrado neste arquivo.

- **Rescue.log**

  Este arquivo tipicamente está localizado no diretório *c:\ibmshare*. Ele fornece informações mais detalhadas que podem ajudar a determinar porque um pacote pode ter falhado, ou para certificar-se de que um pacote funcionou. Ele tem um registro linha por linha daquilo que ocorre em um arquivo zap.

- **Log de Êxito**

  Este arquivo tipicamente é armazenado no diretório *c:\ibmtools\utils\rescue*. Se um arquivo zap encerrou com um valor de zero, ele será registrado aqui.

Exemplo 3

Este exemplo utiliza um site FTP ou HTTP na Área de Pré-Desktop:

1. Defina um Web site externo para os pacotes:

   ```
   ftp.yourmailbox.com
   ```

2. Crie chaves públicas e privadas. Consulte a Etapa 5.
3. Inclua a caixa postal em TVT.TXT

   ```
   mailbox=ftp://nome_do_usuário:senha@ftp.yourmailbox.com
   ```

4. Quando o usuário pressionar IBM/F11 ou a tecla Enter para entrar na Área de Pré-Desktop, o pacote do Antidote Delivery Manager será executado em tempo de inicialização na área de Pré-Desktop.

Exemplo 4

Este exemplo utiliza o arquivo xmltool.exe para destinar a determinados clientes:

1. Distribua o arquivo XML que contém informações que você gostaria de comparar com suas máquinas clientes através do Active Directory, Systems Management Server ou alguma outra ferramenta de gerenciamento.

   ```
   <file>
   <activedirgroup>Marketing</activedirgroup>
   </file>
   ```

2. Na primeira linha do arquivo go.rrs, coloque uma linha que utilize a ferramenta XML. Esta linha é um exemplo que SOMENTE destinaria a máquinas no grupo Marketing:

   ```
   xmltool.exe c:\mycompany\target.xml //file/activedirgroup /c EQU Marketing
   if errorlevel 0 goto RUNIT
   exit errorlevel

   :RUNIT
   #coloque código para executar a correção ou qualquer ação
   ```

Principais Ataques de Worms

O exemplo a seguir demonstra uma possível abordagem para combater um vírus principal. A abordagem básica é desligar a rede, em seguida, reinicializar o Rescue and Recovery, reparar o registro, copiar um arquivo de substituição no local, a inicialização volta ao Windows XP e restaura a rede. Para fins de demonstração, o aplicativo a seguir deve ser atualizado com a sintaxe revisada.

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 has detected a new message \n  \n ..... \n  \n Don't worry; be Happy!
Antidote will fix your system for you" /ok /timer 30
call nettest.cmd %pingtarg%
set el=%errorlevel%
if %el% == 0 msgbox /msg "Network is working" /timer 5 /head "Correct"
if not %el% == 0 msgbox /msg "Network is disabled" /timer 5 /head Failure
NetWk.exe /d
msgbox.exe /msg "Antidote Recovery Process is running. \n  \n Networking has been disabled." /head
"Networking" /timer 15
call nettest.cmd %pingtarg%
set el=%errorlevel%
if %el% == 0 msgbox /msg "Network is working" /timer 5 /head "Failure"
if not %el% == 0 msgbox /msg "Network is disabled" /timer 5 /head "Correct"
msgbox.exe /msg "O sistema reinicializará em 20 segundos \n  \n Pressione OK para reinicializar agora,
ou Cancelar para reinicializar mais tarde."
/head "Select Repair Urgency" /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 "System will apply fix next time you reboot" /head "Reboot" /ok
goto NOT_DONE

:inRR
REM DISABLE NETWORKING
msgbox.exe /msg "Networking will be disabled in 5 seconds. \n  \n  Network disable pending"
/head "Network shutdown" /timer 5
NetWk.exe /d

REM USE EGATHERER VALUES FOR CONDITIONAL BRANCH

msgbox /msg "Checking Registry" /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 "Applying Registry fix. \n  \n Press OK to continue..." /head "Registry Fixeroo" /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 "Registry Now OK \n  \n Applying Fix" /timer 5
copy payload.txt %custos%\

REM RE-ENABLE NETWORK
msgbox.exe /msg "Networking will be enabled in 5 seconds. \n  \n Network enable pending" /head
"Network shutup" /timer 5
NetWk.exe /e

REM TAG IT
echo 1 > %tagfile%

REM REBOOT
msgbox.exe /msg "System will reboot in 5 seconds..." /head "Reboot..." /timer 5
reboot.exe
goto NOT_DONE

:ERROR
:NOT_DONE
exit 1

:DONE
NetWk.exe /e
msgbox.exe /msg "Fix Applied \n  \n You may now continue normal operation."
/head "Done" /ok
exit 0
```

NETTEST.CMD

```
PING –n 1 %1 > nul 2>&
```

PAYLOAD.TXT

```
a test file
of a payload to deliver.
```

Apêndice G. Avisos

É possível que a Lenovo não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte um representante Lenovo local para obter informações sobre produtos e serviços disponíveis atualmente em sua área. Qualquer referência a produtos, programas ou serviços Lenovo não significa que apenas produtos, programas ou serviços Lenovo possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM ou outros direitos legalmente protegidos, poderá ser utilizado em substituição a este produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de qualquer produto, programa ou serviço não-IBM são de responsabilidade do Cliente.

A Lenovo pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento deste documento não garante ao Cliente nenhum direito sobre tais patentes. Pedidos de licença devem ser enviados, por escrito, para:

Lenovo (United States), Inc
500 Park Offices Drive, Hwy 54
Research Triangle Park, NC 27709
USA
Attention: Lenovo Director of Licensing

A LENOVO GROUP LTD. FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO ÀS GARANTIAS IMPLÍCITAS DE NÃO-VIOLAÇÃO, MERCADO OU DE ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em determinadas transações, portanto esta disposição pode não se aplicar ao Cliente.

Esta publicação pode conter imprecisões técnicas ou erros tipográficos. Periodicamente, são feitas alterações nas informações aqui contidas; tais alterações serão incorporadas em novas edições da publicação. A Lenovo pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

Os produtos descritos nesta publicação não são destinados para uso em implantações ou em outras aplicações de suporte à vida, nas quais o mau funcionamento pode resultar em ferimento ou morte. As informações contidas nesta publicação não afetam nem alteram as especificações ou garantias Lenovo. Nada neste documento deverá atuar como uma licença ou isenção expressa ou implícita sob os direitos de propriedade intelectual da Lenovo ou de terceiros. Todas as informações contidas nesta publicação foram obtidas em ambientes específicos e são apresentadas como uma ilustração. O resultado obtido em outros ambientes operacionais pode variar.

A Lenovo pode utilizar ou distribuir as informações fornecidas da forma que julgar apropriada sem incorrer em qualquer obrigação para com o Cliente.

Referências nestas informações a Web sites não-Lenovo são fornecidas apenas por conveniência e não representam de forma alguma um endosso a esses Web sites.

Os materiais contidos nesses Web sites não fazem parte dos materiais deste produto Lenovo e a utilização desses Web sites é de inteira responsabilidade do Cliente

Todos os dados de desempenho aqui contidos foram determinados em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais podem variar significativamente. Algumas medidas podem ter sido tomadas em sistemas de nível de desenvolvimento e não há garantia de que estas medidas serão iguais em sistemas geralmente disponíveis. Além disso, algumas medidas podem ter sido estimadas por extrapolação. Resultados reais podem variar. Os usuários deste documento devem verificar os dados aplicáveis para seu ambiente específico.

Marcas Registradas

Os termos a seguir são marcas registradas da Lenovo nos Estados Unidos e/ou em outros países:

Lenovo
Rescue and Recovery
ThinkPad
ThinkCentre
ThinkVantage
Rapid Restore

Intel é uma marca ou marca registrada da Intel Corporation ou suas subsidiárias nos Estados Unidos e/ou em outros países.

Os termos a seguir são marcas registradas da International Business Machines Corporation nos Estados Unidos e/ou em outros países: IBM, Lotus e Lotus Notes.

Microsoft, Windows e Windows NT são marcas registradas da Microsoft Corporation nos Estados Unidos e/ou em outros países.

Outros nomes de empresas, produtos e serviços podem ser marcas registradas ou marcas de serviço de terceiros.

Glossário

AES (Padrão de Criptografia Avançada). *Padrão de Criptografia Avançada* é uma técnica de criptografia de *chave simétrica*. O governo dos Estados Unidos adotou o algoritmo como sua técnica de criptografia em outubro de 2000, substituindo a criptografia DES que era utilizada. O AES oferece maior segurança contra ataques cruéis do que as chaves DES de 56 bits e o AES pode utilizar chaves de 128, 192 e 256 bits, se for necessário.

Chip de Segurança Embutido. O chip de segurança embutido é outro nome de um Módulo Confiável da Plataforma.

Criptografia de Chave Pública/Chave Assimétrica. Os algoritmos de chave pública geralmente utilizam um par de chaves relacionadas — uma chave é privada e deve ser mantida em segredo, enquanto a outra é tornada pública e pode ser amplamente distribuída; não deverá ser possível deduzir uma chave de um par a partir de outra. A terminologia de ″criptografia de chave pública″ é derivada de uma idéia de fazer parte das informações da chave pública. O termo criptografia de chave assimétrica é também utilizado, pois nem todas as partes contêm as mesmas informações. De certo modo, uma chave ″bloqueia″ uma trava (criptografa); mas uma chave diferente é requerida para desbloqueá-la (decriptografar).

Criptografia de Chave Simétrica. As cifras de criptografia de chave simétrica utilizam a mesma chave para criptografia e decriptografia de dados. As cifras da chave simétrica são mais simples e mais rápidas, mas a principal desvantagem é que as duas partes devem de algum modo trocar a chave de uma maneira segura. A criptografia de chave pública evita esse problema, pois a chave pública pode ser distribuída de uma maneira não-segura e a chave privada nunca é transmitida. O Padrão de Criptografia Avançada é um exemplo de uma chave simétrica.

Senha da BIOS do *Administrador (ThinkCentre)/Supervisor (ThinkPad)***.** A senha do Administrador ou Supervisor é utilizada para controlar a capacidade de alterar as configurações da BIOS. Isso inclui a capacidade de ativar/desativar o chip de segurança embutido e limpar a Chave Raiz de Armazenamento armazenada dentro do Módulo Confiável da Plataforma.

Sistemas Criptográficos. Os sistemas criptográficos podem ser amplamente classificados em criptografia de chave simétrica que utilizam uma única chave que ambos criptografam e decriptografam os dados, e criptografia de chave pública que utiliza duas chaves, uma chave pública conhecida por todos e uma chave privada à qual apenas o proprietário do par de chaves tem acesso.

SRK (Chave Raiz de Armazenamento). A SRK (Chave Raiz de Armazenamento) é um par de chaves públicas de 2.048 bits (ou maior). Ela está inicialmente vazia e é criada quando o proprietário do TPM é designado. Este par de chaves nunca abandona o chip de segurança embutido. Ela é utilizada para criptografar (agrupar) chaves privadas para armazenamento fora do Módulo Confiável da Plataforma e decriptografá-las quando são carregadas novamente no Módulo Confiável da Plataforma. A SRK pode ser limpa por qualquer pessoa que acesse a BIOS.

TPM (Módulo Confiável da Plataforma). Os Módulos Confiáveis da Plataforma são circuitos integrados com finalidade especial construídos nos sistemas para ativar a autenticação clara do usuário e a verificação da máquina. A finalidade principal do TPM é evitar o acesso inadequado a informações confidenciais e sensíveis. O TPM é um hardware baseado em raiz confiável que pode ser alavancado para fornecer uma variedade de serviços criptográficos em um sistema. Outro nome para TPM é o chip de segurança embutido.

ThinkVantage

Impresso em Brazil