ThinkVantage

ThinkVantage 技术部署指南

更新日期: 2005年10月10日

包括:

- Rescue and Recovery V3.0
- 客户端安全解决方案 V6.0
- Fingerprint Software V4.6

ThinkVantage

ThinkVantage 技术部署指南

更新日期: 2005年10月10日

第一版（2005 年 9 月）

目录

前言

本指南面向 IT 管理员或负责在其组织中的计算机上部署 Rescue and Recovery™ 程序的人员。Rescue and Recovery 的目标是通过避免技术支持呼叫和现场支持来降低成本并提高用户效率。它是一种基本工具，使用户和管理员能够在 Microsoft® Windows® 操作系统无法启动或正常运行的情况下复原备份、访问文件、诊断问题并进行以太网连接。它还可以将关键更新部署到受损或未连接到网络的系统，还可以在执行复原时将补丁自动应用到系统。本指南提供在一台或多台计算机上安装 Rescue and Recovery 应用程序所需的信息（前提是每台目标计算机都获得相应的软件许可证）以及该工具多方面的信息（可以通过定制这些信息来支持 IT 或公司策略）。有关使用 Rescue and Recovery 工作空间中包含的不同组件的问题和信息，请参阅组件的联机帮助系统。

Rescue and Recovery 提供功能和应用程序帮助。有关使用 Rescue and Recovery 工作空间中包含的不同组件的问题和信息，请参阅组件的联机帮助系统。

本部署指南由 IT 专业人员编写并对他们遇到的特殊难题进行了阐述。如果您有任何建议或意见，请与您的 Lenovo 授权代表联系。我们将定期更新这些指南，请查看以下 Web 站点以获得后续版本:

www.lenovo.com/ThinkVantage

第 1 章 概述

本指南针对的读者是公司中的 IT 安全人员、管理人员以及负责实施和部署安全技术的其他人员。ThinkVantage™ Rescue and Recovery 代表了一组独特的 ThinkVantage 技术。这个集成型应用程序提供了一套功能强大的工具，即使在 Microsoft® Windows 操作系统无法启动时也可以使用。

在公司环境中，这些技术可以直接和间接地对 IT 专业人员提供帮助。所有 ThinkVantage 技术将使 IT 专业人员获益，因为它们有助于增强个人计算机的易用性和自给自足性，同时提供简化执行的强大工具。ThinkVantage 技术不断帮助 IT 专业人员减少在解决个别计算机问题上耗费的时间，而将更多的时间用于执行核心任务。

主要组成部分

本指南的主要组成部分是:

- ThinkVantage Rescue and Recovery
- ThinkVantage 客户端安全解决方案
- ThinkVantage Fingerprint Software

以下对这三个软件分别进行讨论。

Rescue and Recovery

Rescue and Recovery 包括两个主要组件:

- 即使 Windows 操作系统无法引导，Rescue and Recovery Pre Desktop 环境也能够启动。
- Rescue and Recovery Windows 环境使用户能够对操作系统和文件进行备份、挽救和恢复操作。

注: Rescue and Recovery 的某些功能可以在 Windows 操作系统下运行。在某些情况下，Rescue and Recovery 环境中使用的系统信息是在 Windows 运行时收集的。如果 Windows 操作系统发生故障，则该故障本身不会妨碍 Rescue and Recovery 环境的正常运行。但是，Windows 操作系统下运行的功能是无法配置的，因此本部署指南中并不阐述这些功能。

Rescue and Recovery Pre Desktop 环境

Rescue and Recovery 环境为无法在计算机上启动 Windows 的最终用户提供了一个应急工作空间。该环境在 Windows PE（预安装环境）下运行，它提供 Windows 外观和功能并帮助最终用户在不占用 IT 人员工作时间的情况下解决问题。

Rescue and Recovery 环境主要包含四类功能:

- **挽救和复原**
  - **恢复概述**: 用户可链接到提供的各恢复选项的相关帮助主题。
  - **挽救文件**: 使用户能够将在 Windows 应用程序中创建的文件复制到可移动介质或网络，即便使用被禁用的工作站也能继续工作。

  - **从备份复原**: 使用户能够复原已用 Rescue and Recovery 备份的文件。
- **配置**
  - **配置概述**: 链接到涉及配置的 Rescue and Recovery 环境帮助主题。
  - **恢复密码 / 口令**: 使用户或管理员能够在 Rescue and Recovery 环境中恢复密码或口令。
  - **访问 BIOS**: 打开 BIOS Setup Utility 程序。
- **通信**
  - **通信概述**: 链接到 Rescue and Recovery 环境中的相关帮助主题。
  - **打开浏览器**: 启动 Opera Web 浏览器（Web 或内部网访问需要已连线的以太网连接）。
  - **下载文件**
  - **映射网络驱动器**: 帮助最终用户访问网络驱动器以进行软件下载或文件传输。
- **故障诊断**
  - **诊断概述**: 链接到 Rescue and Recovery 诊断程序帮助主题。
  - **诊断硬件**: 打开可以执行硬件测试并报告结果的 PC Doctor 应用程序。
  - **创建诊断磁盘**
  - **从另一设备引导**
  - **系统信息**: 提供计算机及其硬件组件的相关详细信息。
  - **事件日志**: 提供最近用户活动的详细信息和计算机硬件的列表以帮助确定并解决问题。日志查看器提供一种易读的方式来查看活动和资产日志条目。
  - **保修状态**

预装软件随附的 Lenovo 和 IBM 品牌的个人计算机提供 Rescue and Recovery。它也可以作为可下载文件购买，从而使公司能够在非 Lenovo 和非 IBM 品牌的计算机上得益于 Rescue and Recovery。

第 121 页的附录 B, 『TVT.TXT 设置和值』阐述了如何配置 Rescue and Recovery 环境以进行部署。虽然安装 Rescue and Recovery 包含了 Rapid Restore™ Ultra 的安装，本指南在描述定制、配置和部署时仍将它们视为单独组件。

Rescue and Recovery Windows 环境

Rapid Restore 环境使最终用户按下一个按钮就能挽救丢失的数据、应用程序和操作系统。该功能可以减少耗时的技术支持呼叫，从而节省技术支持成本。

您可以为所有最终用户的计算机调度备份，从而限制风险和停机时间。通过预配置到服务器或外部存储器的自动外部备份，Rescue and Recovery 可以为客户机提供额外的支持。

Antidote Delivery Manager

Antidote Delivery Manager 是 ThinkVantage Rescue and Recovery 中包含的一种反病毒、反蠕虫基础结构。对象易于实现并且有效，此外管理员可以在报告问题后立即启动阻止和恢复。它可以由管理员启动并且可以在未连接到网络的系统上正常使用。Antidote Delivery Manager 补足了现有的反病毒工具而不是取代它们，因此仍需要保留病毒扫描工具并获取补丁。Antidote Delivery Manager 提供了防止破坏和应用补丁的基础结构。

对备份进行加密

缺省情况下，使用 256 AES 密钥对备份进行加密。如果选择安装客户端安全解决方案 V6.0，则可以使用客户端安全解决方案 Gina 进行加密。

客户端安全解决方案 6.0

客户端安全解决方案的主要用途是帮助客户以资产形式保护 PC、保护 PC 上的机密数据以及 PC 访问的网络连接。对于包含可靠计算组织（Trusted Computing Group，TCG）兼容可信平台模块（Trusted Platform Module，TPM）的 IBM® 和 Lenovo 品牌的系统，客户端安全解决方案（CSS）会将该硬件用作系统的信任根。如果系统不包含嵌入式安全芯片，则客户端安全解决方案会将基于软件的密钥用作系统的信任根。客户端安全解决方案 6.0 的功能包括:

- **安全用户认证**

  用户需要一个硬件保护的客户端安全口令才能访问受客户端安全解决方案保护的功能
- **指纹用户认证**

  利用通过 USB 连接的集成指纹技术对用户进行认证，以使用受密码保护的应用程序
- 基于**客户端安全口令／指纹的 Windows 登录**

  要求用户使用硬件保护的客户端安全口令或指纹登录 Windows
- **保护数据**

  通过将敏感文件存储在硬盘驱动器上的安全位置对它们进行加密，这需要有效的用户认证和正确配置的安全芯片
- **管理登录密码**

  安全地管理和存储用户标识和密码等敏感登录信息
- **最终用户密码／口令恢复**

  使用户能够通过回答预配置的问题自行恢复忘记的 Windows 密码／客户端安全口令
- **审计安全性设置**

  使用户能够查看工作站安全性设置的详细列表并做出更改以遵循定义的标准
- **传送数字证书**

  为用户证书和机器证书的私钥提供硬件保护

客户端安全口令

客户端安全口令是用户认证的一种可选附加形式，它可以为客户端安全解决方案应用程序提供增强的安全性。客户端安全口令具有以下需求:

- 长度至少达到八个字符
- 至少包含一个数字
- 与最后三个口令不同
- 包含的重复字符不超过两个
- 不以数字开头

- 不以数字结尾
- 不包含用户标识
- 如果当前口令的使用时间不足三天，则不能更改它
- 不包含当前口令的任何位置中三个或三个以上连续相同的字符
- 与 Windows 密码不同。

客户端安全口令不可接受 Windows 密码可接受的同一攻击类型。必须注意，只有个别用户知道客户端安全口令并且只能利用客户端安全密码恢复功能才能恢复忘记的客户端安全口令。如果用户忘记了恢复问题的答案，则无法恢复客户端安全口令保护的数据。

客户端安全密码恢复

这个可选设置使登记的用户能通过正确回答三个问题来恢复忘记的 Windows 密码或客户端安全口令。如果启用该功能，每个用户在最终用户客户端安全登记过程中需要为十个预选问题选择三个答案。如果用户忘记了 Windows 密码或客户端安全口令，通过回答这三个问题即可自行重新设置他们的密码或口令。

注:

1. 使用客户端安全口令时，这是恢复忘记的口令的唯一方法。如果用户忘记了这三个问题的答案，该用户就必须重新运行登记向导并且先前受到客户端安全保护的所有数据将丢失。
2. 使用客户端安全来保护 Rescue and Recovery Pre Desktop 环境时，“密码恢复”选项实际将显示用户的客户端安全口令和 / 或 Windows 密码。这是因为 Pre Desktop 环境不能自动执行 Windows 密码更改操作。如果未连接到网络、本地高速缓存的域用户在登录 Windows 时执行该功能，情况也是这样。

ThinkVantage Fingerprint Software

Lenovo 提供的生物测定指纹技术旨在帮助客户降低密码管理的相关成本、增强系统的安全性并遵循条例。与我们的指纹识别器配合使用，ThinkVantage Fingerprint Software 可以向 PC 和网络进行指纹认证。该解决方案还可以与客户端安全解决方案 V6.0 集成以提供扩展功能。您可以通过以下地址进一步了解 Lenovo 指纹技术并下载该软件:

www.thinkpad.com/fingerprint

ThinkVantage Fingerprint Software 提供以下功能:

- **客户机软件功能**
  - **取代 Microsoft Windows 密码**

    用指纹取而代之，以实现简便、快速而安全的系统访问。
  - **更换 BIOS（又称为开机密码）和硬盘驱动器密码**。

    用指纹取代这些密码，以增强登录安全性和简便性。
  - **滑动手指即可访问 Windows**:

    用户在启动时只需滑动一下手指即可访问 BIOS 和 Windows，从而节省宝贵的时间。

- **与客户端安全解决方案集成**以用于 CSS 密码管理器并利用可信平台模块。用户只需滑动手指即可访问 Web 站点和特定应用程序。

• **管理员功能**
  - **切换安全方式**:

    管理员可以在安全方式与便捷方式之间切换以修改受限用户的访问权。
  - **管理控制台**:

    通过脚本驱动的命令行界面启用 Fingerprint Software 的远程软件定制，从而帮助管理员进行操作。

• **安全功能**
  - **软件安全性**:

    将用户模板存储在系统中或将它们从识别器传送到软件时，通过强加密来保护它们。
  - **硬件安全性**:

    识别器具有一个安全协处理器，它用于存储并保护指纹模板、BIOS 密码和加密密钥。

密码管理器

客户端安全密码管理器使您能够管理并记住所有敏感、易忘的应用程序和 Web 站点登录信息，如用户标识、密码和其他个人信息。客户端安全密码管理器通过嵌入式安全芯片存储所有信息，这样对应用程序和 Web 站点的访问始终是高度安全的。

这意味着您不必记住和提供大量单独的密码（这些密码都符合不同的规则和有效期），而只需记住一个密码／口令、提供您的指纹或识别元素的组合即可。

客户端安全密码管理器使您能够执行以下功能:

• **通过嵌入式安全芯片对所有已存储的信息进行加密**

  客户端安全密码管理器通过嵌入式安全芯片自动对所有信息进行加密。这确保了您所有的敏感密码信息将受到客户端安全解决方案加密密钥的保护。

• **利用简单的输入和传送界面来快速和方便地传送用户标识和密码**

  客户端安全密码管理器输入和传送界面使您能够将信息直接放入浏览器或应用程序的登录界面中。这有助于将输入错误降至最低并使您能够通过嵌入式安全芯片安全地保存所有信息。

• **自动键入用户标识和密码**

  客户端安全密码管理器实现了登录过程的自动化，当您访问登录信息已输入客户端安全密码管理器中的应用程序或 Web 站点时，就会自动输入您的登录信息。

• **生成随机密码**

  客户端安全密码管理器使您能够为每个应用程序或 Web 站点生成随机密码。这使您能够提高数据的安全性，因为每个应用程序都将启用更为严格的密码保护。随机密码的安全性远高于用户定义的密码，因为经验表明大多数用户都将易于记忆的个人信息作为密码，而这样的密码通常比较容易破解。

- **使用客户端安全密码管理器界面编辑记录**

  客户端安全密码管理器使您能够在一个简单易用的界面中编辑所有的帐户记录并设置所有的可选密码功能。这使得密码和个人信息管理变得快捷而方便。

- **从 Microsoft(R) Windows(R) 桌面上的图标栏或通过简单的键盘快捷方式来访问登录信息**

  每当您需要将另一个应用程序或 Web 站点添加到密码管理器时，密码管理器图标使您能够轻松访问登录信息。还可以通过简单的键盘快捷方式方便地访问每个客户端安全密码管理器功能。

- **导出和导入登录信息**

  客户端安全密码管理器使您能够导出敏感的登录信息，以便在计算机之间安全地传递该信息。从客户端安全密码管理器导出登录信息时会创建一个受密码保护的导出文件，该文件可以存储在可移动介质上。无论您身在何处都可以使用该文件访问您的用户信息和密码，或使用密码管理器将记录导入另一台计算机中。

  注: 导入功能只能用于客户端安全解决方案 V6.0。客户端安全解决方案 V5.4X 和先前版本无法导入客户端安全解决方案 6.0 密码管理器。

SafeGuard PrivateDisk

使用 SafeGuard PrivateDisk 保护数据。几乎所有人都会在 PC 上存储机密数据。SafeGuard PrivateDisk 可以保护机密数据。对于您的计算机、所有磁盘驱动器和移动介质上的机密和宝贵信息，它就像一个 “电子保险箱”。未授权的人员无法访问或读取受保护的信息。

SafeGuard PrivateDisk 的工作原理是什么？SafeGuard PrivateDisk 以虚拟盘原理（Virtual Disk Principle）为基础。

- 可以在任何可用的驱动器上创建虚拟盘
  - 移动内存介质（如磁盘、USB 棒、CD-ROM、DVD 或 Zip 驱动器）
  - 硬盘，网络驱动器
- 驱动程序的操作方法与磁盘驱动器相同
  - 操作系统将读写命令透明地发送给驱动程序。
  - 驱动程序管理加密的存储器。
  - 对所有数据和目录信息进行加密。
- SafeGuard PrivateDisk 与客户端安全解决方案及可信平台模块一同保护 PrivateDisk 生成的数字证书
- SafeGuard PrivateDisk 对每个虚拟盘使用一种对称密码算法（带有一个新的随机 AES 密钥）
  - AES、128 位、CBC 方式
  - 为每个虚拟盘提供一个新的随机密钥
- 认证途径:
  - 密码
  - 私钥（X.509 证书），智能卡（可选）
  - 可以使用自动生成的 EFS 证书

- 密码安全性:
  - PKCS#5
  - 提供错误的密码后的延时
  - 与“拦截保护”的密码对话框

Security Advisor

Security Advisor 工具使您能够查看计算机上当前设置的安全性设置的摘要。您可以查看这些设置来了解当前的安全性状态或增强系统安全性。包含的部分安全性主题是硬件密码、Windows 用户密码、Windows 密码策略、受保护的屏幕保护程序以及文件共享。可以通过 TVT.txt 文件来更改显示的类别缺省值。

证书转移向导

客户端安全证书转移向导指导您逐步完成转移与证书关联的私钥的过程，即将该私钥从基于软件的 Microsoft 加密服务提供程序（CSP）转移到基于硬件的客户端安全解决方案 CSP。在转移后，由于私钥受到嵌入式安全芯片的保护，所以使用证书的操作将更安全。

Hardware Password Reset

该工具创建一个独立于 Windows 运行的安全环境并帮助您重新设置忘记的开机密码和硬盘驱动器密码。通过回答您创建的一组问题来确定您的身份。最好在忘记密码之前，尽快创建这个安全环境。只有当您在硬盘驱动器上创建该安全环境并登记后，才能重新设置忘记的硬件密码。只有特定 ThinkCentre® 和 ThinkPad 计算机上提供这个工具。

支持没有可信平台模块的系统

客户端安全解决方案 6.0 现在支持没有兼容的嵌入式安全芯片的 IBM 和 Lenovo 品牌的系统。这样即可在整个企业范围内进行标准安装，从而创建一个同质安全环境。具有嵌入式安全硬件的系统抵御攻击的能力更强；而只有软件保护的机器也能得益于附加的安全性和功能。

系统迁移辅助程序

系统迁移辅助程序（SMA）是一个软件工具，系统管理员可以使用它将用户的工作环境从一个系统迁移到另一个系统中。用户的工作环境包括以下内容:

- 操作系统首选项（如桌面和网络连接设置）
- 文件和文件夹
- 定制应用程序设置（如 Web 浏览器中的书签或 Microsoft Word 中的编辑首选项）
- 用户帐户

系统管理员可以使用 SMA 为公司设置一个标准的工作环境或升级个别用户的计算机。个别用户可以使用 SMA 对计算机进行备份或将设置和文件从一个计算机系统迁移到另一个计算机系统。例如，从一台台式计算机迁移到一台移动式计算机（膝上型计算机）。

OEM 区别

OEM 系统上暂时不提供客户端安全解决方案 6.0。Rescue and Recovery 不会利用 OEM 机器上的任何客户端安全解决方案应用程序。

第 2 章 安装注意事项

在安装 ThinkVantage Rescue and Recovery 之前，您必须了解整个应用程序的体系结构。

Rescue and Recovery

Rescue and Recovery 有两个主要界面。主界面在 Windows XP 或 Windows 2000 环境中运行。辅助界面（Rescue and Recovery Pre Desktop 环境）则独立于 Windows XP 或 Windows 2000 操作系统，在 Windows PE 环境中运行。

注:

1. 仅当先安装 Rescue and Recovery、后安装 Computrace 时，Rescue and Recovery 可用于非 BIOS 版本的 Computrace。请参阅第 97 页的第 8 章，『最佳做法』。
2. 如果您试图在装有 Rescue and Recovery 的系统上安装 SMS 并且已经将 Windows PE 区域作为虚拟分区安装，将无法安装 SMS。因为 Windows PE 和 SMS 都将 C:\minint 目录作为其文件系统。要同时安装它们，就必须将 Rescue and Recovery 2.0 作为 12 型分区进行安装。有关安装到 12 型分区的说明，请参阅第 109 页的『将 Rescue and Recovery 安装到 12 型服务分区中』。
3. 在装有 Rescue and Recovery 的系统上安装 Microsoft Recovery Console 可能带来潜在的安全风险。Microsoft Recovery Console 查找带有路径 C:*\system32\config\ 的所有文件夹，并在找到该路径时假定它是操作系统。如果需要 Windows 密码的注册表项不存在，则 Recovery Console 将允许用户选择操作系统，然后可以访问整个硬盘驱动器而无需输入密码。

覆盖安装注意事项

Rescue and Recovery V3.0 支持对 Rescue and Recovery 2.0 进行覆盖安装。

建议在安装 Rescue and Recovery 3.0 后制作一个新的备份。该操作可以使用脚本或用户界面完成。

以下是获得一个干净的备份集所要遵循的基本步骤:

1. 将先前的备份复制到 CD/DVD 驱动器或 USB HDD 驱动器（如果需要）
2. 删除当前备份
3. 执行基本备份

以下脚本首先将备份复制到 USB HDD，然后删除当前备份，最后执行基本备份。

```
@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
```

客户端安全解决方案

部署客户端安全解决方案 6.0 时，必须考虑到以下几个方面。

客户端安全解决方案在代码中包含了必要的驱动程序和软件支持，以启用接收客户端安全解决方案 6.0 的机器的安全硬件（可信平台模块）。启用硬件至少需要一次重新引导，因为芯片实际是通过 BIOS 控制的并且需要 BIOS 认证成功才能完成该过程。换言之，如果设置了 BIOS 管理员／超级用户密码，则需要用该密码来启用／禁用可信平台模块。

在可信平台模块可以执行任何功能之前，首先必须初始化“所有权”。每个系统有且只有一个控制客户端安全解决方案选项的客户端安全解决方案管理员。该管理员必须具有 Windows 管理员特权。可以使用 XML 部署脚本来初始化管理员。

完成系统所有权的配置后，将自动提示登录系统的其他各个 Windows 用户完成客户端安全安装向导，从而登记并初始化用户的安全密钥和安全证书。

可信平台模块的软件仿真

客户端安全解决方案可以在没有可信平台模块的限定系统上运行。该功能与可信平台模块的唯一区别在于它将使用基于软件的密钥而不是使用受硬件保护的密钥，其他则完全相同。该软件还可以安装一个开关，以强制其始终使用基于软件的密钥而不是利用可信平台模块。这是一个安装时的决策，并且只有在卸载并重新安装软件之后才能撤销。

以下是强制可信平台模块的软件仿真的语法:

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

升级方案

有关从先前级别的客户端安全解决方案进行升级的信息，请参阅第 87 页的『已安装软件的情况』。

第 3 章 Rescue and Recovery 定制

本章提供可用于定制 ThinkVantage Rescue and Recovery 的信息。

用桌面上的“创建基本备份”图标生成简单部署

在开始该过程之前，请确保一个或多个 TVT 文件（如 z062zaa1025us00.tvt）与可执行文件或 MSI 文件位于同一目录中，否则安装将失败。如果文件名为 setup_tvtrnr3_1027**c**.exe，则下载的是组合程序包。这些说明适用于可从*大企业单独语言文件*下载页面单独下载的文件。

要执行在桌面上为用户放置备份图标的简单部署，请执行以下操作:

1. 将 SETUP_TVTRNR*XXXX*.EXE（其中 *XXXX* 为构建标识）解压缩到一个临时目录中:

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

2. 根据需要，定制 TVT.TXT 文件。例如，您可能要在每个星期二的下午 3:00 调度一次每周备份。在 TVT.TXT 的 [Rescue and Recovery] 节中添加以下条目完成定制。（有关其他设置信息，请参阅第 121 页的附录 B, 『TVT.TXT 设置和值』。）

   ```
   ScheduleHour=15

   ScheduleMinute=00

   ScheduleDayOfTheWeek=2
   ```

3. 并将 Z062ZAA1025US00.TVT 文件复制到 C:\tvtrr。这个 TVT 文件必须与 MSI 文件位于同一文件夹中。
4. 启动 MSI 安装并将重新引导延后:

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

   注: 上述命令为适合本页而修改。将这个命令作为一个字符串输入。
5. 定制 Rescue and Recovery 环境。（有关详细信息，请参阅第 17 页的『Predesktop Area』。）
6. 删除 C:\TVTRR 目录中的临时文件。（请参阅第 14 页的『Windows 环境』）。
7. 撰写带有以下命令的命令文件:

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

   注: 上述命令为适合本页而修改。将这个命令作为一个字符串输入。
8. 在所有用户桌面上创建名为“创建基本备份”的快捷方式。（在该项目的**输入位置**下指定路径。）
9. 在系统上运行 Sysprep 实用程序。
10. 创建部署映像。

在客户机用户接收到映像并将计算机个性化后，用户单击**创建基本备份**图标以启动 Rescue and Recovery 并保存基本备份。

捕获基本备份中的 Sysprep 映像

要捕获基本备份中的 Sysprep 实用程序映像，请执行以下操作:

1. 执行管理安装:

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

2. 将以下节添加到 C:\TVTRR\Program Files\IBM ThinkVantage\Rescue and Recovery 中的 TVT.TXT 文件的末尾:

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

3. 使用 MSIEXE 文件安装 Rescue and Recovery:
   a. 对于所有 MSI，添加以下安装日志生成代码:

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

   b. 要使用 MSIEXE 文件安装这些安装文件，请输入以下命令:

```
: Perform the install of Rescue and Recovery

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

   c. 要使用 MSIEXE 静默安装这些安装文件:

   输入以下命令（最后重新引导）:

```
: 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
```

   输入以下命令（禁止重新引导）:

```
: 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. 输入以下命令:

```
: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"
```

   如果要使用密码，请添加语法 password=*pass*。

5. 看到以下消息时，请运行特定的 Sysprep 实施:

```
************************************************
** 已准备好制作 sysprep 备份。                  **
** 请立即运行 SYSPREP 并关机。                  **
**                                              **
```

```
** 下次引导机器时，它将引导至                    **
** PreDesktop Area 并制作备份。                  **
************************************************
```

6. 当 Sysprep 完成时，关闭并重新引导机器。

   注: 操作系统将重新引导并进入 Rescue and Recovery 的 PreDesktop Area。您将看到状态栏显示**正在进行系统复原**。
7. 完成时，您将看到状态栏显示消息**Sysprep 备份完成**。
8. 使用电源按钮关闭系统电源。
9. 捕获部署映像。

在 Sysprep 备份中捕获多个分区机器和排除文件

要在 Sysprep 实用程序备份中捕获多个分区，请执行以下操作:

1. 执行管理安装:

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

2. 将以下节添加到 C:\\”Program Files”\″ IBM ThinkVantage\Rescue and Recovery″:\tvtrr\ 中的 TVT.TXT 文件的末尾:

   ```
   [Backup0]
   BackupVersion=2.0

   [BackupDisk]
   CustomPartitions=0
   ```

   要 “排除” 某个分区，请将以下节添加到 TVT.TXT 文件中:

   ```
   [BackupDisk]
   CustomPartitions=1

   [PartitionX].
   IncludeInBackup=0
   ```

   其中 **X** 是分区号
3. 如果要从备份中排除 .MPG 和 .JPG 文件，请将它们添加到 IBMFILTER.TXT 中，如下例所示:

   ```
   X=*.JPG
   X=*.MPG
   ```
4. 使用 MSIEXE 安装 Rescue and Recovery:
   a. 对于所有 MSI，添加以下安装日志生成代码:

      ```
      /L*v %temp%\rrinstall.txt
      ```
   b. 要使用 MSIEXE 安装这些安装文件，请输入以下命令:

      ```
      : Perform the install of Rescue and Recovery

       msiexec /i "C:\TVTRR\Rescue and Recovery - Client Security Solutiion.msi"
      ```
   c. 要使用 MSIEXE 静默安装这些安装文件:

      输入以下命令（最后重新引导）:

```
: 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
```

输入以下命令（禁止重新引导）：

```
: 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. 输入以下命令:

```
: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"
```

如果要使用密码，请添加语法 password=*pass*。

6. 看到以下消息时，请运行特定的 Sysprep 实施:

```
************************************************
** 已准备好制作 sysprep 备份。                 **
** 请立即运行 SYSPREP 并关机。                 **
**                                            **
** 下次引导机器时，它将引导至                  **
** PreDesktop Area 并制作备份。                **
************************************************
```

7. 当 Sysprep 完成时，关闭并重新引导机器。

   注: 操作系统将重新引导并进入 Rescue and Recovery 的 PreDesktop Area。您将看到状态栏显示**正在进行系统复原**。

8. 完成时，您将看到状态栏显示消息**Sysprep 备份完成**。
9. 使用电源按钮关闭系统电源。
10. 捕获部署映像。

Windows 环境

在备份中包含和排除文件

Rescue and Recovery 具有广泛的包含和排除能力。它可以包含和排除个别文件、文件夹或整个分区。

控制包含和排除功能的文件按优先顺序如下列出。所有文件位于 C:\program files\ibm thinkvantage\rescue and recovery 目录中。

1. IBMFILTER.TXT
2. GUIEXCLD.TXT

缺省情况下，最终用户可以选择要从备份中排除的个别文件和文件夹。这些文件和文件夹存储在文件 GUIEXCLD.TXT 中。

如果管理员要确保始终备份某个特定文件或文件夹，则该管理员可以将文件名或文件类型包含在 IBMIFILTER.TXT 文件中。无论 GUIEXCLD.TXT 中的条目如何，该文件中的任何条目将始终包含在备份中。

管理员还能够始终从备份中排除文件、文件夹或分区。

始终从任何备份中排除以下文件和文件夹:
- PAGEFILE.SYS
- HIBERFILE.SYS
- C:\SYSTEM VOLUME INFORMATION

复原后，Windows 将自动重新生成 PAGEFILE.SYS 和 HIBERFILE.SYS。另外，Windows 将在复原备份后重新生成 Windows 系统复原数据（带有一个新的复原点）。

IBMFILTER.TXT

文件格式为:
- 每个包含 / 排除规则条目占一行。
- 如果将多个规则应用于一个文件或文件夹，则应用最后一个规则。文件底部的条目优先级最高。
- 条目必须以下列某个符号或字母开头:
  - **;**

    用于注释
  - **I**

    必须包含与条目匹配的文件或文件夹
  - **X**

    必须排除与条目匹配的文件或文件夹
  - **S**

    必须包含文件或文件夹上的单实例存储（Single Instance Storage）
  - **i**

    用于可以选择包含的文件或文件夹
  - **x**

    用于可以选择排除的文件或文件夹
  - **s**

    用于将文件或文件夹识别为通常包含的单实例存储（可选）。

```
 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=?:\Program Files\*
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
```

定制 Rescue and Recovery 的其他方面

您可以使用名为 TVT.TXT 的外部文件（该文件在安装过程之前已定义）来定制 Rescue and Recovery 的诸多方面。该 TVT.TXT 文件位于 C:\Program Files\IBM ThinkVantage\ 子目录中。

该 TVT.TXT 文件将遵循标准的 Windows INI 文件格式，其数据按节（用 [] 表示）组织并且每行一个条目，如下所示:

```
setting=value
```

例如，如果不要对所有备份数据进行加密，请在 TVT.TXT 文件中包含以下行:

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

位于 EncryptBackupData 之后的参数 0 指示 Rescue and Recovery 不对备份进行加密。

第 121 页的附录 B, 『TVT.TXT 设置和值』中描述了 TVT.TXT 中 [Rescue and Recovery] 节的设置字符串、参数和缺省设置的完整列表。

故障凭单

目前没有办法通过 FTP 或电子邮件从 Rescue and Recovery 环境自动传输；将指示最终用户使用浏览器中集成的电子邮件以及要传输的文件的位置。不支持动态数据传输，但记录功能将把日志事件打包到一个文件中并指示用户可以通过电子邮件发送的程序包位置和文件名。这将创建 *Req 115 Trouble Ticket* XML 文件，该文件提供了系统信息（Current® HW、eGatherer 和 PCDR 诊断记录信息）中显示的所有信息，它将放在 Rescue and Recovery 环境和操作系统 – C:\IBMSHARE 都可以轻松找到和访问的位置。

Diagnostics 是 PreDesktop Area 提供的一个基本应用程序，它可以帮助您确定问题。这些测试的输出内容将得到妥善保存，以便查看或将其传送给技术支持。Rescue and Recovery 将提供多个工具，以恢复到用户先前备份的 Windows 环境版本。

Rescue and Recovery 包含将用户分区完整复原为先前版本的工具以及恢复个别文件的工具。这些工具将提供对用户数据的备份的访问权。它们将提供对这些数据进行完整或部分恢复的能力。

OSFILTER.TXT

该文件可在不影响用户数据的情况下恢复操作系统和应用程序。Rescue and Recovery 通过使用显式枚举和通配符过滤提供了有选择地复原特定文件和文件夹（包括子文件夹）的能力，同时不会删除任何其他数据。一个外部文件将定义组成操作系统和应用程序的文件、文件夹或文件类型（利用通配符）。该文件可以由管理员定制并提供一个缺省外部文件。当用户选择恢复操作系统时，将显示一个菜单，允许他们使用以下 Windows 选项进行 “部分复原”：仅复原与这个外部文件中包含的规则匹配的文件。管理员可以定制这个外部文件的内容。

要查看 OSFILTER.TXT 文件，请使用以下路径：`cd %RR%`。有关文件格式的信息，请参阅第 15 页的『IBMFILTER.TXT』。

Predesktop Area

要定制 Rescue and Recovery PreDesktop Area 的各个部分（即使操作系统未打开，它也可以启动），请使用 RRUTIL.exe 实用程序来获取（GET）和放置（PUT）文件。下表列出了这些文件及其定制选项:

表 1. RRUTIL.exe 文件和定制选项

文件 / 目录	定制选项
\MININT\SYSTEM32 WINBOM.INI	添加静态 IP 地址，更改视频分辨率
\MININT\INF \MININT\SYSTEM32\DRIVERS	添加设备驱动程序
MAINBK.BMP	修改环境背景
MINIMAL_TOOLBAR(1).INI	禁用地址栏
NORM1.INI	配置 Opera 浏览器、禁用 Opera 地址栏、更改 Opera 代理设置、指定固定的下载目录、向可下载文件列表添加特定的文件扩展名以及更改具有特定扩展名的文件的行为
OPERA_010.CMD	排除 Windows 用户的收藏夹
OPERA6.INI	配置 Opera 浏览器，禁用地址栏

表 1. RRUTIL.exe 文件和定制选项 (续)

文件 / 目录	定制选项
PEACCESS*xx*.INI（其中 *xx* 为指定的语言）	预引导环境: 主 GUI 字体、环境背景、左右面板条目和功能以及基于 HTML 的帮助系统
STANDARD_MENU.INI	启用显示“另存为”窗口

使用 RRUTIL.EXE

您可以从包含本文档的 Web 站点获取 RRUTIL.EXE 以及在本指南中提到的其他实用程序。

以下过程列出了从 Rescue and Recovery 环境获取（GET）文件并将文件放置（PUT）到其中的步骤。这些步骤适用于 Rescue and Recovery 环境的所有文件定制。

要使用 RRUTIL.EXE，请执行以下操作:

1. 将 RRUTIL.exe 复制到 C 盘根目录下。
2. 用以下语法创建 GETLIST.TXT 文件:

   `\preboot\usrintfc\`*`file name`*

   将文件另存为 C:\TEMP\GETLIST.TXT。
3. 在命令提示符处，输入 RRUTIL.exe 命令以及下表中定义的某个开关。然后使用相应的参数完成命令，如下表所示。

表 2. 命令和开关选项

命令和开关选项	结果
`RRUTIL -l1`	列出预引导目录的内容
`RRUTIL -l2`	列出 minint 目录的内容
`RRUTIL -l4`	列出 C 盘根目录或 12 型分区根目录的内容
`RRUTIL -g C:\temp\getlist.txt C:\temp`	从预引导分区获取文件
`RRUTIL -d C:\temp\ dellist.txt`	从预引导分区删除文件
`RRUTIL -p C:\temp`	在预引导分区中添加或替换文件
`RRUTIL -r` *`path \oldname.ext newname.ext`* `RRUTIL -r \temp\rr\test.txt test2.txt`（文件位于 preboot\rr 目录中）	在 PreDesktop Area 中重命名文件
`RRUTIL -bp C:\temp`	在 RRBACKUPS 虚拟分区中更新或替换文件
`RRUTIL -bl` *`path`* RRUTIL -bl lists to `C:\rr-list.txt` `rrutil -bl c:\rrtemp`	列出 RRBACKUPS 目录
`RRUTIL -br RRbackups\C\n`（其中“n”是备份编号）	删除备份的内容
`RRUTIL -bg C:\temp\bgetlist.txt C:\temp`	从 \RRBACKUPS 复制个别文件
`RRUTIL -s`	RRBACKUPS 占用的空间

4. 当您执行“GET”例程后，可以使用标准文本编辑器来编辑文件。

示例: PEACCESSIBMxx.INI

该示例名为 PEACCESSIBM*xx*.INI，您可以通过这个配置文件来定制 Rescue and Recovery 环境的各个元素（请参阅第 20 页的『定制预引导环境』）。

注: 文件名中的 *xx* 表示以下某个两字母语言缩写:

表 3. 语言码

两字母语言码	语言
br	巴西葡萄牙语
dk	丹麦语
en	英语
fi	芬兰语
fr	法语
gr	德语
it	意大利语
jp	日语
kr	韩国语
nl	荷兰语
no	挪威语
po	葡萄牙语
sc	简体中文
sp	西班牙语
sv	瑞典语
tc	繁体中文

从 Rescue and Recovery 环境获取文件 PEACCESSIBMEN.INI:

1. 使用以下参数创建 GETLIST.TXT 文件:

   ```
   \preboot\reboot\usrintfc\PEAccessIBMen.ini
   ```

2. 将文件另存为 C:\TEMP\GETLIST.TXT。
3. 在命令提示符处输入以下命令:

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

将文件 PEACCESSIBMEN.INI 放回 Rescue and Recovery 环境中。在命令行发出以下命令:

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

注: “PUT”（**-p**）例程使用“GET”（**-g**）例程中创建的目录结构。为了正确放置编辑过的文件，请确保编辑过的文件位于和 GETLIST.TXT 文件中建立的相同目录中，如下例所示:

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

示例: 向 PreDesktop Area 添加设备驱动程序

1. 从供应商的 Web 站点或其他介质获取设备驱动程序。
2. 创建以下目录结构:

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

   ```
   C:\TEMP\MININT\SYSTEM32\DRIVERS
   ```

3. 将所有网络驱动程序 *.INF 文件复制到 MININT\INF 目录。（例如，E100B325.INF 需要位于 \MININT\INF 目录中。）

4. 将所有 *.SYS 文件复制到 \MININT\SYSTEM32\DRIVERS 目录。（例如，E100B325.SYS 需要位于 MININT\SYSTEM32\DRIVERS 目录中。）
5. 将任何相关的 *.DLL、*.EXE 或其他文件复制到 \MININT\SYSTEM32\DRIVERS 目录中。（例如，E100B325.DIN 或 INTELNIC.DLL 文件必须位于 MININT\SYSTEM32\DRIVERS 目录中。）

   注:
   a. 目录文件不是必要文件，因为 Rescue and Recovery 环境不处理这些文件。上述说明适用于配置计算机可能需要的任何设备驱动程序。
   b. 由于 Windows Professional Edition 的限制，您可能必须根据注册表的更新情况手动应用一些配置应用程序或设置。
6. 要将设备驱动程序放入 Rescue and Recovery 环境中，请在命令行输入以下命令:

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

定制预引导环境

通过编辑配置文件 PEACCESSIBM*xx*.INI（其中 *xx* 为指定的语言），您可以定制 Rescue and Recovery 环境的以下元素:

- 主 GUI 字体
- 环境背景
- 用户界面的左面板中的条目和功能
- Rescue and Recovery 环境的基于 HTML 的帮助系统

注: 要获取、编辑和替换 PEACCESSIBMEN.INI 文件，请参阅第 19 页的『示例: PEACCESSIBMxx.INI』。

更改主 GUI 字体

您可以更改主图形用户界面（GUI）的字体。缺省设置可能无法正确显示所有字符（取决于所需的语言和字符）。在 PEACCESSIBM*xx*.INI（其中 *xx* 为指定的语言）中，[Fonts] 节包含显示的字符样式的缺省设置。以下是大多数单字节字符集语言的缺省设置:

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

根据您的视觉和字符集的需求，以下字体与 Rescue and Recovery 环境兼容。其他字体可能兼容，但未经测试:

- Courier
- Times New Roman
- Comic Sans MS

更改环境背景

右面板的背景是位于 \PREBOOT\USRINTFC 目录中的位图 MAINBK.BMP。如果您为右面板背景创建您自己的位图图像，则它必须符合以下尺寸:

- 620 像素宽
- 506 像素高

您必须将该文件放在 \PREBOOT\USRINTFC 目录中，使 Rescue and Recovery 能呈现所需的背景。

注: 要获取、编辑和替换 MAINBK.BMP 文件，请参阅第 18 页的『使用 RRUTIL.EXE』。

更改左面板中的条目和功能

更改左面板条目需要编辑 PEACCESSIBM*xx*.INI 文件（其中 *xx* 为指定的语言）。有关从 Rescue and Recovery 环境获取 PEACCESSIBM*xx*.INI 以及替换该文件的信息，请参阅第 18 页的『使用 RRUTIL.EXE』。

Rescue and Recovery 的左面板中有 21 个条目。虽然功能不同，但每一个都具有相同的基本元素。以下是左面板条目的示例:

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

表 4. 左面板条目和定制选项

条目	定制选项
00-01	完全可定制。
02	必须保留按钮类型 1（请参阅表 5）。可以更改文本。可以定义应用程序或帮助功能。无图标可添加。
03-06	完全可定制。
07	必须保留类型 1。可以更改文本。可以定义应用程序或帮助功能。无图标可添加。
08-10	完全可定制。
11	必须保留按钮类型 1。可以更改文本。可以定义应用程序或帮助功能。无图标可添加。
16	必须保留类型 1。可以更改文本。可以定义应用程序或帮助功能。无图标可添加。
17–22	完全可定制。

定义条目类型: **Button00** 必须是唯一标识。编号确定了左面板中按钮的显示顺序。

Button00=[0-8] 该参数确定了按钮类型。该编号可以是 0 到 8 之间的一个整数。下表说明类型和每个按钮类型的工作情况:

表 5. 条目类型参数

参数	按钮类型
0	空字段。要将行保留为空白和未使用时，请使用该值。
1	节首文本。使用该设置建立主要分组或节首。
2	应用程序启动。定义当用户单击按钮或文本时启动的应用程序或命令文件。
3	Rescue and Recovery 环境的 Opera 帮助。定义使用 Opera 浏览器时启动的帮助主题。
4	启动前显示重新启动消息窗口。使用这些值指示 GUI 向用户显示消息，表明在执行指定功能之前必须重新启动计算机。
5	保留供 Lenovo Group Ltd 使用
6	保留供 Lenovo Group Ltd 使用
7	启动和等待。该说明后的字段强制环境在继续之前等待已启动的应用程序提供的返回码。返回码需要在环境变量 %errorlevel% 中。

表 5. 条目类型参数 (续)

参数	按钮类型
8	启动应用程序。GUI 在启动应用程序之前检索国家或地区代码和语言。它用于具有 CGI 脚本的 Web 链接以从某个国家或地区或者以某种语言打开 Web 页面。
9	保留供 Lenovo Group Ltd 使用
10	保留供 Lenovo Group Ltd 使用

定义条目字段:

Button00=[0-10], "title"

按钮类型参数后的文本指定按钮的文本或标题。如果文本超出左面板的宽度，将截断该文本并以省略号表示后面还有更多字符。使用悬浮式帮助时将显示完整的标题文本。

Button00=[0-10], "title", file.bmp

在标题文本后，指定要用作图标的位图的文件名（该图标用于即将创建的按钮）。该位图不能超出 15 x 15 像素以确保大小合适。

Button00=[0-10], "title", file.bmp, [0 or 1]

该设置指示环境显示或隐藏条目。值 0 隐藏条目。如果将值设置为 0，则显示空行。值 1 显示条目。

Button00=[0-10], "title", file.bmp, [0 or 1], 1

这是一个保留功能，必须始终设置为 1。

Button00=[0-10], "title", file.bmp, [0 or 1], 1, [0 or 1]

要在启动应用程序之前要求提供密码，请在此处输入值 1。如果将该值设置为 0，则在启动指定的应用程序之前不需要提供密码。

Button00=[0-10], "title", file.bmp, [0 or 1], 1, [0 or 1], %sysdrive%[pathname\executable]

%sysdrive@ 的值必须是引导驱动器盘符。在引导驱动器盘符后，您必须为应用程序或命令文件提供标准路径。

Button00=[0-10], "title", file.bmp, [0 or 1], 1, [0 or 1],%sysdrive%[pathname\executable], [parameters]

提供将启动的目标应用程序所需的任意数量的参数。

如果您没有提供各字段的值，则必须提供必要的逗号以便于按钮定义可以接受并正确地运行。例如，如果您正在创建组头 “Rescue and Recover”，则以下将是条目代码:

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

条目 02、07、11 和 16 必须保持类型 0（或头部分）条目，并且始终落入它们的数字位置。可以通过将完全可定制条目设置为类型 0（左面板中的空行）来降低落入头部分以下的条目的可用性。但是，条目的总数不能超出 23。

下表显示可以从左面板条目启动的功能和可执行文件:

表 6. 左面板功能和可执行文件

功能	可执行文件
恢复文件	WIZRR.EXE

表 6. 左面板功能和可执行文件 (续)

功能	可执行文件
从备份复原	WIZRR.EXE
创建迁移文件	WIZRR.EXE
打开浏览器	OPERA.EXE
映射网络驱动器	MAPDRV.EXE
诊断硬件	RDIAGS.CMD; 启动 PC Dr 应用程序（仅限 IBM 和 Lenovo 品牌的预装型号）
创建诊断软盘	DDIAGS.CMD

更改右面板中的条目和功能

更改右面板条目需要编辑 PEACCESSIBM*xx*.INI 文件（其中 *xx* 为指定的语言）。有关从 Rescue and Recovery 环境获取 PEACCESSIBM*xx*.INI 以及替换该文件的信息，请参阅第 19 页的『示例: PEACCESSIBMxx.INI』。

右面板的功能链接、用户消息和窗口状态是可定制的。

定制右面板中的功能链接: 要更改横跨右面板顶部的链接的功能，请修改 PEACCESSIBM*xx*.INI（其中 *xx* 为指定的语言）的 [TitleBar] 节。这些链接与左面板条目的操作方式相同。按钮编号值是 00 到 04。可以从左面板启动的应用程序同样也可以从 [TitleBar] 条目启动。有关可以从标题栏启动的可执行文件的完整列表，请参阅第 18 页的『使用 RRUTIL.EXE』。

修改用户消息和窗口状态: PEACCESSIBM*xx*.INI（其中 *xx* 为指定的语言）包含两个节，您可以修改其中向用户显示的消息:

```
[Welcome window]

[Reboot messages]
```

PEACCESSIBM*xx*.INI（其中 *xx* 为指定的语言）中的 [Welcome] 节定义了“欢迎”窗口。根据对左面板做出的更改，您可以更改标题行以及行 01 到 12 中的信息。您可以设置用来显示标题、头以及粗体字的字体:

```
[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)"
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"
```

以下设置用于用户界面上的“标题栏帮助”功能:

Command0

为基本帮助页面启动的 HTML 页面

Command1

Lenovo 许可证协议 HTML 页面

HELP 帮助

LICENSE

许可证

CANCEL

取消

Command0

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

Command1

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

要完全隐藏“欢迎”窗口，请将 `NoShowCk=0` 更改为 `NoShowCk=1`。要更改标题和欢迎文本的显示字体，请根据您的设计首选项编辑该节的最后三行内容。

注: 请勿更改或删除行 13 和 14。

在 PEACCESSIBM*xx*.INI 文件（其中 *xx* 为指定的语言）的 [REBOOT] 节中，您可以修改以下行中的值:

```
NoShowChk=

RebootText=
```

“NoShowChk”的两个值为 `0` 和 `1`。当用户选择时，可以隐藏该消息。当显示消息时用户单击复选框，值将设置为 `0`。要显示消息，请将值更改为 `1`。如果需要，可以更改 [REBOOT] 节中消息的字体。例如，该值可以设置如下:

```
RebootText = "Arial"
```

注: PEACCESSIBM*xx*.INI 文件（其中 *xx* 为指定的语言）中的以下节可用，但它们不可以定制: [Messages]、[EXITMSG] 和 [HelpDlg]。

配置 Opera 浏览器

Opera 浏览器有两个配置文件，其中一个包含缺省配置。另一个是“活动”配置。最终用户可以更改活动配置，但重新启动 Rescue and Recovery 后所作更改将丢失。

要对浏览器做出永久更改，请编辑位于 %systemdrive%，C 上文件夹路径 C:\PREBOOT\OPERA\PROFILE 中的 OPERA6.INI 和 NORM1.INI 的副本。OPERA6.INI 的临时“活动”副本位于 ramdrive (Z:) 上的 Z:\PREBOOT\OPERA\PROFILE 目录中。

注:

1. 要获取、编辑和替换 OPERA6.INI 及 NORM1.INI 文件，请参阅第 18 页的『使用 RRUTIL.EXE』。
2. Opera 工作空间经过修改可提供增强的安全性。因此，已删除某些浏览器功能。

电子邮件

Rescue and Recovery 通过 Opera 浏览器提供基于 Web 的电子邮件支持。Opera 提供基于 IMAP 的电子邮件（可以通过大型企业配置启用），但它不受支持。要获取有关如何启用它的参考信息，请阅读位于以下地址的 “System Administrator’s Handbook”：

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

禁用地址栏

要禁用 Opera 中的地址栏，请完成以下过程:

1. 通过使用第 18 页的『使用 RRUTIL.EXE』中描述的 RRUTIL 过程，从 C:\PREBOOT\OPERA\PROFILE\TOOLBAR 获取文件 MINIMAL_TOOLBAR(1).INI。
2. 打开要编辑的文件。
3. 找到文件的 [Document Toolbar] 节。
4. 找到 “Address0” 条目。
5. 将分号（; – 注释定界符）置于 “Address0” 条目前。

   注: 在此停止并继续步骤 7 将禁用 Opera 工具栏，但将保留不具备功能的 “Go” 按钮和工具栏图形。要删除 “Go” 按钮和工具栏，请继续步骤 6。
6. 找到以下条目，然后将分号置于每个条目前:

   ```
   Button1, 21197=Go Zoom2
   ```
7. 保存文件。
8. 通过使用第 18 页的『使用 RRUTIL.EXE』中描述的 RRUTIL 过程放置文件。当运行 Opera 时，将禁用地址栏。

定制书签

Opera 浏览器配置为读取 ramdrive 文件 Z:\OPERADEF6.ADR 中建立的书签。根据启动例程中的代码启动 Rescue and Recovery 时，将生成该文件。启动例程自动导入 Windows Internet Explorer 书签并添加一些其他书签。因为启动时生成的 ramdrive 文件是暂时的，所以请将书签添加到 Internet Explorer，当启动 Rescue and Recovery 环境时将自动导入该文件。

您可以排除部分或全部 Internet Explorer 收藏夹。要排除特定 Windows 用户的收藏夹，请执行以下操作:

1. 通过使用第 18 页的『使用 RRUTIL.EXE』中描述的 RRUTIL 过程获取 C:\PREBOOT\STARTUP\OPERA_010.CMD。
2. 打开要编辑的文件。
3. 在 .CMD 文件中找到以下行: PYTHON.EXE.FAVS.PYC Z:\OPERADEF6.ADR
4. 在该代码行的末尾输入要排除其收藏夹的 Windows 用户的名称（以引号括起）。例如，如果要排除 “所有用户” 和 “管理员” 的收藏夹，则代码行如下:

   ```
   python.exe favs.pyc z:\Operadef6.adr "All Users, Administrator"
   ```
5. 保存文件。
6. 通过使用第 18 页的『使用 RRUTIL.EXE』中描述的 RRUTIL 过程放置文件。

如果不要在 Rescue and Recovery 环境提供的浏览器中显示任何 Internet Explorer 收藏夹，请执行以下操作:

1. 通过使用第 18 页的『使用 RRUTIL.EXE』中描述的 RRUTIL 过程获取 C:\PREBOOT\STARTUP\OPERA_010.CMD 以进行编辑。
2. 在 .CMD 文件中找到以下行: PYTHON.EXE.FAVS.PYC Z:\OPERADEF6.ADR
3. 执行以下某个操作:
   a. 在行首输入 REM，如下:

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

   b. 删除文件中的代码行。
4. 保存文件。
5. 通过使用第 18 页的『使用 RRUTIL.EXE』中描述的 RRUTIL 过程将文件放回原位置。

更改代理设置

要更改 Opera 浏览器的代理设置，请执行以下操作:

1. 通过使用第 18 页的『使用 RRUTIL.EXE』中描述的 RRUTIL 过程获取文件 C:\PREBOOT\OPERA\PROFILE\NORM1.INI 以进行编辑。
2. 将以下节添加到 NORM1.INI 文件的末尾:

   注: [0 or 1] 变量表示检查项为启用（1）或禁用（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. 保存文件。
4. 通过使用第 18 页的『使用 RRUTIL.EXE』中描述的 RRUTIL 过程将文件放回原位置。

要添加 HTTP、HTTPS、FTP、Gopher 或 WAIS 代理，请在相应的行之后输入 =<address of proxy>。例如，如果您的代理服务器地址是 http://www.your company.com/proxy，则 HTTP 服务器行如下:

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

要向条目添加端口，请在地址后输入冒号并输入端口号。对于 “No Proxy Servers” 和 “Automatic Proxy Configuration URL” 字段，操作相同。

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

启用或指定完整的下载路径

有多个设置可供操作以启用显示“另存为”窗口。最简单的方法是:

1. 通过使用第 18 页的『使用 RRUTIL.EXE』中描述的 RRUTIL 过程获取 C:\PREBOOT\OPERA\DEFAULTS\STANDARD_MENU.INI 文件。
2. 在 [Link Popup Menu] 节中，找到以下字符串:

   ```
   ;;Item, 50761
   ```

3. 删除两个分号，然后保存文件。关闭并重新打开 Rescue and Recovery 时，最终用户即可右键单击链接并且将显示“目标另存为”选项。这样即可显示“另存为”窗口。

   注: 直接链接（非重定向的链接）适用于以上过程。例如，如果某个链接指向一个 .PHP 脚本，则 Opera 只保存该脚本（而不是该脚本指向的文件）。
4. 通过使用第 18 页的『使用 RRUTIL.EXE』中描述的 RRUTIL 过程将文件放回原目录结构。

要指定一个固定的下载目录，请执行以下操作:

1. 使用第 18 页的『使用 RRUTIL.EXE』中描述的 RRUTIL 过程获取 C:\PREBOOT\OPERA\NORM1.INI 文件。
2. 在文件中，找到以下行:

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

3. 将 %OpShare% 更改为目录的完整路径，您要用该目录来保存下载的文件。
4. 保存 NORM1.INI 文件。关闭并重新打开 Rescue and Recovery 时，Opera 将下载的文件保存到指定的目录。
5. 通过使用第 18 页的『使用 RRUTIL.EXE』中描述的 RRUTIL 过程将文件放回原位置。

注:

1. 定制下载的完整路径并不使用户能够保存目标文件（即使链接已重定向）。
2. Opera 浏览器配置为仅下载 .ZIP、.EXE 和 .TXT 文件类型并且只为这些文件类型更改 Opera 行为。（可能有成千上万的文件类型使用三字母的文件扩展名。正如 Rescue and Recovery 环境并不是用于取代 Windows 环境，Opera 浏览器也不是用于取代功能完善的浏览器。提供因特网访问以帮助用户筹备和运行。识别的文件类型的数量需要限制。对于挽救和恢复用途，.ZIP、.EXE 和 .TXT 文件应该足够。如果要传输另一个文件类型，最好是创建一个随后可以解压缩的 .ZIP 文件。）
3. 文件类型通过 mime 类型识别（而不是通过文件扩展名）。例如，如果某个 .TXT 文件以 .EUY 作为扩展名命名，该文件在 Opera 浏览器中仍作为文本文件打开。

将特定的文件扩展名添加到可下载的文件列表

您可以向文件列表添加可通过 Rescue and Recovery 浏览器下载的文件的扩展名。要向列表添加扩展名，请完成以下过程:

1. 确保 Opera 和所有 Opera 窗口（包括 Rescue and Recovery 帮助文件）都已关闭。
2. 使用第 18 页的『使用 RRUTIL.EXE』中描述的 RRUTIL 过程获取 C:\PREBOOT\OPERA\NORM1.INI 文件。
3. 找到文件的 [File Types] 节。
4. 使用搜索功能查看所需的文件扩展名是否已列出，但不起作用；然后请执行以下某个操作:
   - 如果找到扩展名，但带有该扩展名的文件无法正确使用，请完成以下步骤:

a. 将扩展名后的值由 8 更改为 1。（值 8 指示浏览器忽略该文件。值 1 指示浏览器保存该文件。）例如，将以下:

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

更改为

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

b. 滚动到 NORM1.INI 文件的 [File Types Extension] 节，然后搜索文件的 mime 类型。例如，找到 VIDEO/MPEG=,8

c. 将 ,8 值更改为:

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

注: 如果已设置指定的值，请勿更改该值。

d. 保存文件，然后将该文件复制到 OPERA6.INI，随后重新启动 Rescue and Recovery 以使更改生效。

- 如果扩展名不存在并且所需类型的文件无法正确使用，请执行以下操作:
  a. 在 NORM1.INI 的 [File Types Extension] 节，找到临时 mime 条目。以下为示例: temporary=1,,,,lwp,prz,mwp,mas,smc,dgm,|
  b. 将文件类型扩展名添加到列表。例如，如果要添加 .CAB 作为识别的扩展名，则根据以下样本条目添加:

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

注: 尾随的逗号和管道符号对于使该设置生效很关键。如果省略了任何一个，则列表中的所有文件扩展名可能都将被禁用。

  c. 将文件保存到目录路径 C:\TEMP\。
  d. 将文件复制到 OPERA6.INI。
  e. 重新启动 Rescue and Recovery 工作空间以使更改生效。

更改带有特定扩展名的文件的工作情况

您可以通过替换 NORM1.INI 文件中的值更改文件的工作情况。要通过扩展名更改文件工作情况，请执行以下操作:

1. 关闭 Opera 及所有活动的 Opera 窗口（包括帮助文件）。
2. 通过使用第 18 页的『使用 RRUTIL.EXE』中描述的 RRUTIL 过程打开 PREBOOT\OPERA\NORM1.INI 文件以进行编辑。
3. 找到文件的 [File Types] 节，然后搜索要操作的扩展名。例如，要将所有 .TXT 文件保存到 IBMSHARE 文件夹。
4. 找到以下条目: TEXT/PLAIN=2,,,,TXT,|

   注: 值 2 指示浏览器在 Opera 中显示文本。值 1 指示浏览器将目标文件保存在 IBMSHARE 文件夹中。
5. 继续以 .TXT 为例，将行更改为以下内容:

```
TEXT/PLAIN=1,,,,TXT,|
```

6. 通过使用第 18 页的『使用 RRUTIL.EXE』中描述的 RRUTIL 过程保存文件并将它放回原位置。
7. 重新启动 Rescue and Recovery 工作空间以使更改生效。

添加静态 IP 地址

要添加静态 IP 地址，需要更改以下文件。

1. 通过使用第 18 页的『使用 RRUTIL.EXE』中描述的 RRUTIL 过程获取 \MININT\SYSTEM32 WINBOM.INI 文件。
2. 在 WINBOM.INI 文件中，将 [WinPE.Net] 节添加到 [PnPDriverUpdate] 之前。例如，考虑以下文件: WINBOM.INI

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

   必须将以下行添加到 [WinPE.Net] 节中。

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

表 7. 静态 IP 地址条目

条目	描述
Gateway	指定 IP 路由器的 IP 地址。配置缺省网关在 IP 路由表中创建缺省路由。 **语法:** Gateway = *xxx.xxx.xxx.xxx*
IPConfig	指定 Windows PE 用于连接到网络的 IP 地址。 **语法:** IPConfig = *xxx.xxx.xxx.xxx*
StartNet	指定是否启动联网服务。 **语法:** StartNet = *Yes* | *No*
SubnetMask	指定一个 32 位值，该值使 IP 包的收件人能够区别 IP 地址的网络标识和主机标识部分。 **语法:** SubnetMask = *xxx.xxx.xxx.xxx*

3. 通过使用第 18 页的『使用 RRUTIL.EXE』中描述的 RRUTIL 过程获取 PREBOOT\IBMWORK NETSTART.TBI 文件。
4. 将

   ```
   factory -minint
   ```

   更改为

   ```
   factory -winpe
   ```
5. 注释掉以下行:

```
regsvr32 /s netcfgx.dll

netcfg -v -winpe

net start dhcp

net start nla
```

6. 通过使用第 18 页的『使用 RRUTIL.EXE』中描述的 RRUTIL 过程将 \IBMWORK NETSTART.TBI 和 \MININT\SYSTEM32 WINBOM.INI 文件放回原位置。

更改视频分辨率

您可以通过更改缺省 predesktop 分辨率的设置（800 × 600 × 16 位）更改视频分辨率。要更改设置，请执行以下操作:

1. 通过使用第 18 页的『使用 RRUTIL.EXE』中描述的 RRUTIL 过程获取 MININT\SYSTEM32\WINBOM.INI 文件。
2. 在文件 WINBOM.INI 中添加以下条目:

   ```
   [ComputerSettings]

   DisplayResolution=800x600x16 or 1024x768x16

   In the file preboot\ibmwork\netstart.tbi change factory-minint to factory-winpe
   ```

   当 Rescue and Recovery 环境启动时，您在启动过程中将看到标题为“出厂预装”的附加窗口。并且颜色将由数千色降至 256 色。
3. 通过使用第 18 页的『使用 RRUTIL.EXE』中描述的 RRUTIL 过程将 MININT\SYSTEM32\WINBOM.INI 文件放回原位置。

启动应用程序

Rescue and Recovery Windows PE 环境能够支持启动脚本、程序或定制程序。将在 Rescue and Recovery Windows PE 环境到达主 PE 界面页之前处理这些脚本或程序。

放置脚本或程序的目录是 Preboot\Startup。将按照字母数字顺序处理该目录中的脚本或程序。因此，将在 1.EXE 之前处理名为 A.BAT 的脚本。

要将脚本或程序放入该目录中，请执行以下操作:

1. 从位于以下地址的 Lenovo Rescue and Recovery “管理工具” 站点获取 RRUTIL:

   www.lenovo.com/ThinkVantage
2. 创建一个 Temp 目录
3. 在 \Temp 目录中创建以下目录树: \preboot\startup
4. 将脚本或程序放入 \temp\preboot\startup 路径中
5. 在命令行中输入 RRUTIL –p \Temp
6. 要验证是否已成功复制脚本或程序，请在命令行中输入 RRUTIL –g。这将生成一个名为 getlist.txt 的文件。
7. 检查 \preboot\startup 目录中 getlist.txt 的内容。该树下应列出脚本或程序。

密码

PreDesktop Area 中提供四个密码选项。它们是:

- PreDesktop 密码或主密码
- 用户标识和密码或口令

- 备份密码
- 无密码

PreDesktop 密码或主密码

您可以设置一个独立的 PreDesktop Area 密码。该密码通过命令行界面设置，如果未安装客户端安全解决方案，它将成为唯一可用的密码选项。

您可以使用以下命令创建这个 PreDesktop Area 密码: C:\Program Files\IBM ThinkVantage\Client Security Solution\pe_setupmasterpwde.exe。

该命令的参数为:

表 8.

参数	描述
create password	该参数创建实际密码。
verify password	该参数验证密码是否有效并且可以使用。
change currentPassword *newPassword*	该参数允许您将当前密码更改为另一个密码。
exists	该参数检查密码是否存在。
silent	该参数隐藏所有消息。
setmode values	0 = 不需要认证 1 = 需要特定于用户的认证 2 = 需要主密码

注: 受限用户无法更改密码；管理员可以为受限用户重新设置密码。

用户标识和密码或口令

该选项将客户端安全解决方案代码用于密码或口令管理。客户端安全登录在启动 PreDesktop Area 时将提示用户输入该密码或口令。这为多用户环境提供了更高的安全性。如果用户使用 GINA 登录，则该用户只能访问自己的文件，而不能访问其他用户的文件。

该选项可以由 CSS GUI 或通过 XML 脚本设置。

备份密码

备份密码可以通过 GUI “设置密码” 或命令行界面 “rrcmd” （需指定备份）设置。以下是一些示例:

```
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
```

无密码

该选项不使用认证，它允许用户在不使用密码的情况下进入 PreDesktop Area。

标识密码访问

密码访问有三个选项:

- 主密码

- 用户标识和密码或口令
- 无密码

主密码

主密码是单个密码，它允许您访问 PreDesktop Area 和备份。它通过使用命令行界面设置，如果未安装客户端安全解决方案，它将成为唯一的密码选项。

用户标识和密码或口令

该选项将客户端安全解决方案代码用于密码或口令管理。客户端安全解决方案 GINA 在启动 PreDesktop Area 时将提示用户输入该密码或口令。这为多用户环境提供了更高的安全性。如果用户使用 GINA 登录，则该用户只能访问自己的文件，而不能访问他人的文件。

注: 这还包括用户的 SecureDrive PrivateDisk 加密卷文件中的信息。

该选项可以通过命令行界面或 GUI 设置。

无密码

该选项不使用认证，它允许用户在不使用密码的情况下进入 PreDesktop Area。

复原类型

以下是复原文件的各种方法:

- 文件挽救
- 单一文件复原
- 操作系统和应用程序
- 系统重生
- 完整复原
- 出厂内容 / Image Ultra Builder

注: Rescue and Recovery 无法在复原后为域用户捕获高速缓存的安全证书。

文件挽救（在任何复原之前）

该功能提示用户提供备份存储位置，然后由用户选择一个备份。接着，ThinkVantage Rescue and Recovery 应显示该用户登录后有权访问的文件。接着由用户选择要挽救的文件和 / 或文件夹。随后，系统显示可以将文件挽救到的位置（本地 HDD 除外）。用户选择一个具有足够空间的目标并由系统复原文件。

单一文件复原

该功能提示用户提供备份存储位置，然后由用户选择一个备份。接着，ThinkVantage Rescue and Recovery 应显示该用户登录后有权访问的文件。接着由用户选择要复原的文件和 / 或文件夹，系统将它们复原到其原位置。

操作系统和应用程序

该功能使用户能够选择一个备份，然后系统将删除 osfilter.txt 中的规则定义的文件。然后从选定的备份复原 OSFILTER.TXT 定义的文件。tvt.txt 文件中还有选项可指定某个程序在复原前或复原后运行，请参阅第 121 页的附录 B, 『TVT.TXT 设置和值』中的 TVT 设置和值。

注:

1. 操作系统和应用程序始终使用 “密码持久性”。
2. CD/DVD 备份不提供操作系统和应用程序复原。

您可以添加在备份和复原前后运行的定制任务。有关备份和复原设置，请参阅第 121 页的附录 B, 『TVT.TXT 设置和值』。

系统重生

当您选择对系统进行系统重生时，Rescue and Recovery 程序将通过制作一个新的增量备份并对硬盘驱动器和备份进行碎片整理来优化系统性能。然后，它从您选择的备份复原选定的设置和数据。在维护当前设置和数据时，系统重生操作有助于消除病毒、广告软件和间谍软件。该操作可能比较耗时。

要对系统进行系统重生，请完成以下过程:

1. 从 Rescue and Recovery 界面中，单击**从备份复原系统**图标。显示 “复原系统” 屏幕。
2. 在 “复原系统” 屏幕上，选择**对系统进行系统重生**。
3. 通过完成以下过程来选择要用于对系统进行系统重生的驱动器和备份:
   a. 从可用驱动器的下拉菜单中选择适当的驱动器。Rescue and Recovery 界面将显示选定驱动器上的备份文件。
   b. 选择要用于对系统进行系统重生的备份文件。
   c. 单击**下一步**。
   d. 确认选定的备份是要用于对系统进行系统重生的备份，然后单击**下一步**开始复原过程。将提醒您切勿在这一操作过程中关闭计算机电源。
   e. 单击**确定**继续。显示一个进度条。该操作比较耗时。

您可以添加在系统重生之前或之后运行的定制任务。有关系统重生设置，请参阅第 121 页的附录 B, 『TVT.TXT 设置和值』。

注: 创建选定的备份后安装或卸载的应用程序可能需要再次安装才能正常使用。
警告: 在启动备份、复原、系统重生或归档过程之前，请确保已将系统连接到交流电源。否则可能导致数据丢失或不可恢复的系统故障。

完整复原

该功能删除本地驱动器上的所有文件，然后从选定的备份复原文件。如果选择密码持久性，将复原最新的可用密码。

出厂内容 / Image Ultra Builder（IUB）

该功能擦除硬盘并重新安装所有出厂预装软件。

密码持久性

下表列出了决定是否使用“密码持久性”时的注意事项。

表 9. 密码持久性注意事项

问题	启用“密码持久性”时的影响
如果用户使用当前帐户和密码登录旧的备份，则无法使用任何已加密文件系统的文件和文件夹，因为那些文件是针对原来的帐户和密码加密的，而不是针对持久帐户和密码加密的。	• 用户将丢失已加密文件系统的数据 • 已加密文件系统和密码持久性不能同时使用。
如果特定备份上不存在该用户，则用户没有任何“用户文件夹”或文件。所有 Internet Explorer 收藏夹和应用程序数据都不存在。	• 用户标识文档设置将丢失 • 可能丢失数据
在当前帐户和密码中删除用户将从所有备份中除去他们的认证信息。	• 用户将无法访问数据
如果经理或网络管理员要删除几位前雇员的访问权并复原为基本备份，以便重置系统以除去所有雇员认证帐户，则雇员仍可以使用“密码持久性”进行访问。	• 违背 Microsoft 用户标识维护惯例及建议。

从本地硬盘驱动器复原时，如果选择“密码持久性”，将使用当前密码。从 USB 或网络复原时，将使用最新备份的密码。

Hardware Password Reset

Hardware Password Reset 环境独立于 Windows 运行并允许您重新设置忘记的开机密码和硬盘驱动器密码。通过回答您在登记时创建的一组问题来确定您的身份。最好在忘记密码之前，尽快创建、安装并登记这个安全环境。只有在登记之后，您才能重新设置忘记的硬件密码。只有特定 ThinkCentre™ 和 ThinkPad 计算机支持这一恢复介质。

创建该环境无法帮助您恢复忘记的 Windows 密码或与 Rescue and Recovery 工作空间关联的密码。创建该环境将在“Startup Device”菜单中添加一个附加可引导设备，您可以使用它来重新设置忘记的硬件密码。当提示输入开机密码时，您可以按 F12 访问该菜单。

设置密码部署涉及三个阶段:

1. 程序包构建
2. 程序包部署
3. 登记

在开始本过程之前，请在 BIOS 中设置管理员或超级用户密码。如果您还未设置 BIOS 管理员或超级用户密码，您的环境还不够安全。准备部署密码重新设置程序包的所有系统都必须具有超级用户密码。完成该过程后，开机密码与硬盘驱动器密码将相同。该过程旨在帮助您完成创建安全环境的任务并帮助您在创建安全环境后重新设置忘记的密码。

程序包构建

要创建安全环境，请执行以下操作:

1. 在 Hardware Password Reset 安装应用程序中，选中“创建安全环境以重新设置硬件密码”单选按钮。
2. 单击“确定”。 “BIOS 超级用户密码”窗口打开。
3. 在“输入超级用户密码”字段中，输入您的管理员或超级用户密码。这是您先前在 BIOS 中设置的用于保护硬件设置的管理员或超级用户密码。
4. 单击“确定”。 “创建密钥”窗口打开。
5. 在“密钥生成”区域中，请执行以下某个操作:

   第一次创建这个安全环境时，您必须创建一个新密钥。密钥是一种用于认证您的身份的安全功能部件。对于任何后续安全环境的创建尝试，您可以选择使用第一次尝试时创建的相同密钥（如果选择导出它）或创建一个不同的密钥。如果只为一台计算机创建该环境，最好生成一个新密钥。您可以选择在每次构建新的安全操作系统时生成一个密钥。但是，该选项要求您在每台机器上重新执行登记过程。如果使用相同的密钥，则不必重新执行登记。如果要为多台计算机创建该环境，您可能希望使用相同的密钥。但是，如果要使用相同的密钥，建议您务必妥善保存该密钥。

   在“密钥生成”区域，请执行以下某个操作:

   - 如果这是您第一次创建密钥并且您只准备在这台计算机上创建安全环境，请选中“生成新密钥”单选按钮。
   - 如果这是您第一次创建密钥并且您要创建一个可部署到其他计算机的安全环境，请选中“生成新密钥”单选按钮。然后选中“将密钥导出到文件”复选框。使用“浏览”按钮来定义要存储密钥的位置。
   - 如果您已经创建了一个密钥并且要使用它来创建可部署到其他计算机的安全环境，请选中“从文件导入密钥”单选按钮。使用“浏览”按钮来定义要使用的密钥的位置。您将需要在以上选项中创建的密钥。

   当部署到 Thinkpad 和 Thinkcentre 时，为每种受支持的系统并根据语言（如法语、德语和日语）设置一个提供者系统。其目的是保护操作系统，操作系统取决于 Rescue and Recovery 分区并且每个系统各不相同。
6. 在安装区域中，取消选中“创建后自动安装 Hardware Password Reset”复选框。
7. 单击**确定**。
8. 当对话框指示您运行安装程序包后才能在这台计算机上启用“Hardware Password”功能时，请单击**确定**。

   要找到可执行文件的路径，请在命令行提示处输入 cd %rr%\rrcd\passwordreset\pwdreset.exe。

程序包部署

使用公司的现有分发介质来部署创建的程序包。

登记

要登记 Password Reset，请执行以下操作:

1. 运行 pwdreset.exe。
2. 单击“确定”以重新启动计算机。计算机将重新启动并提示您输入 BIOS 密码。输入您的 BIOS 密码，然后单击 **Enter 键**。计算机将重新启动并进入安全环境中并且“欢迎使用 Hardware Password Reset”窗口打开。

3. 如果这是您第一次创建安全环境或是要重新登记计算机和硬盘，请选中**设置硬件重新设置**单选按钮。
4. 单击**下一步**。“硬盘设置”窗口打开。
5. 在“计算机序列号”区域中，选中要设置的计算机一侧的“设置”复选框。
6. 单击**下一步**。“输入新的开机密码”窗口打开。
7. 在**新的开机密码**字段中，输入要使用的开机密码。如果已经有一个开机密码，将把它重新设置为您在该字段中输入的密码。另外，您的硬盘驱动器密码也将设置为相同的密码。
8. 单击**下一步**。“创建安全问题和答案”窗口打开。
9. 在三个问题字段中，分别输入要使用的问题。
10. 在三个答案字段中，分别输入每个问题的答案。如果您忘记了开机密码并试图对它进行重新设置，您必须知道每个答案。
11. 单击**下一步**，然后单击**完成**。将在 Windows 环境中重新启动计算机。

以下是 Hardware Password Reset 安装程序的错误消息。前两个是普通标题，它们与其余消息结合使用。两种情况下都建议您重新安装产品。

- **IDS_STRING_ERR** “错误”
- **IDS_STRING_ERR_INT** “内部错误”
- **IDS_STRING_ERR_CMDLINE** “无法识别您输入的命令行选项。\n\n用法: scinstall [/postenroll | /biosreset | /newplanar]”
- **IDS_STRING_ERR_NOTSUPPORTED**

  该计算机不支持 Hardware Password Reset。
- **IDS_STRING_ERR_MEM**

  该计算机没有足够的内存运行 Hardware Password Reset 功能。
- **IDS_STRING_ERR_ENVAR**

  缺少必需的环境变量。必须安装 Rescue and Recovery 3.0（或更高版本）才能使用 Hardware Password Reset 功能。
- **IDS_STRING_ERR_MISSINGDLL**

  缺少必需的 DLL。必须安装 Rescue and Recovery 3.0（或更高版本）才能使用 Hardware Password Reset 功能。
- **IDS_STRING_ERR_BIOSMAILBOX**

  为安装 Hardware Password Reset 功能而进行的 BIOS 更新失败。请关闭计算机；然后重新启动并重试 Hardware Password Reset 安装。
- **IDS_STRING_ERR_INSTALLRETRY**

  未成功完成该操作。要重试，请关闭并重新启动计算机，然后再次运行 Hardware Password Reset 安装。
- **IDS_STRING_ERR_INSTALLPUNT**

  未成功完成该操作。要对问题进行故障诊断，请咨询系统管理员或查看 Rescue and Recovery 文档以获得详细信息。

第 4 章 客户端安全解决方案定制

本章使用可靠计算组织（TCG）定义的可信平台模块方面的术语。有关这些术语更详细的说明，请访问以下站点以获得参考资料和定义:

http://www.trustedcomputinggroup.org/

嵌入式安全芯片 / 可信平台模块的优点

可信平台模块是一枚嵌入式安全芯片，旨在为利用它的软件提供与安全性相关的功能。嵌入式安全芯片安装在系统的主板上并通过硬件总线进行通信。采用可信平台模块的系统可以创建密钥并对它们进行加密，这样只有相同的可信平台模块才能对它们进行解密。该过程通常称为将密钥*打包*，它有助于防止密钥泄露。在具有可信平台模块的系统上，名为“存储根密钥（SRK）”的主打包密钥存储在可信平台模块本身中，这样始终不会泄露密钥的私有部分。嵌入式安全芯片还可以存储其他存储密钥、签名密钥、密码和其他小数据单元。但是可信平台模块中的存储容量有限，因此 SRK 用于对其他密钥进行加密以实现芯片外存储。由于 SRK 始终不离开嵌入式安全芯片，它构成了受保护存储区的基础。

当需要可信平台模块保护的数据时，受保护的数据将传送到安全的嵌入式硬件环境中进行处理。成功完成认证和解密后，便可在系统中使用不受保护的数据。

任何硬件对攻击的抵御能力都比软件强，采用可信平台模块的系统在这一方面也不例外。利用密钥时，这一点尤为重要。非对称密钥对的私有部分与操作系统控制的内存保持分离。可信平台模块使用自己的内部固件和逻辑电路来处理指令，既不依赖于操作系统，也不会受外部软件漏洞的影响。

任何系统都无法提供十全十美的安全性，采用可信平台模块技术的系统也不例外。嵌入式安全芯片设计用于抵御篡改或电子分析。但是，执行揭开可信平台模块保护的机密所需的分析需要对机器的物理访问和其他专用硬件，这使得支持嵌入式安全芯片的平台上的机密比只有软件保护的系统上的机密更安全。增加从系统窃取机密的难度有助于提高个人或企业的整体安全级别。

使用嵌入式安全芯片是一个可选过程并且需要一个客户端安全解决方案管理员。无论对于个别用户还是公司 IT 部门，都必须初始化可信平台模块。从硬盘驱动器故障或替换的系统板恢复等后续操作也必须由客户端安全解决方案管理员执行。

客户端安全解决方案如何管理密钥

客户端安全解决方案的内部运作可以用两个主要部署活动来描述: 获取所有权和登记用户。第一次运行客户端安全安装向导时，在初始化过程中将执行“获取所有权”和“登记用户”过程。完成客户端安全安装向导的特殊 Windows 用户标识是客户端安全解决方案管理员并且登记为活动用户。将自动要求登录系统的每个其他用户登记到客户端安全解决方案中。

- **获取所有权 – 指定客户端安全解决方案管理员**

将指定一个 Windows 管理员用户标识作为系统唯一的客户端安全解决方案管理员。必须通过该用户标识执行客户端安全解决方案管理功能。可信平台模块权限是该用户的 Windows 密码或客户端安全口令。

注：从忘记的客户端安全解决方案管理员密码或口令恢复的唯一方法是用有效的 Windows 权限卸载软件或清除 BIOS 中的安全芯片。无论选择哪种方法，通过与可信平台模块关联的密钥保护的数据都将丢失。客户端安全解决方案还提供一个可选机制，它允许用户根据问答式提问应答（这是“登记用户”功能的一部分）自行恢复忘记的密码或口令。由客户端安全解决方案管理员决定是否使用该功能。

- **登记用户**

  一旦完成“获取所有权”过程并创建了客户端安全解决方案管理员，就可以创建一个“用户基本密钥”以安全地存储当前已登录的 Windows 用户的安全证书。这一设计可使多个用户登记客户端安全解决方案并利用一个可信平台模块。用户密钥通过安全芯片获得保护，但它们实际并不是存储在芯片上而是存储在硬盘驱动器上。与其他安全技术不同，这一设计创建硬盘驱动器空间作为有限的存储因子而不是使用安全芯片中构建的实际内存。这一设计可以大幅度增加利用同一安全硬件的用户的数量。

获取所有权

客户端安全解决方案的信任根是系统根密钥（System Root Key，SRK）。这个不可迁移的非对称密钥是在可信平台模块的安全环境中生成的并且始终不会向系统公开。利用该密钥的权限是在“TPM_TakeOwnership”命令期间通过 Windows 管理员帐户获得的。如果系统使用的是客户端安全口令，则客户端安全解决方案管理员的客户端安全口令将作为可信平台模块权限，否则使用客户端安全解决方案管理员的 Windows 密码。

系统级别密钥结构 — 获取所有权

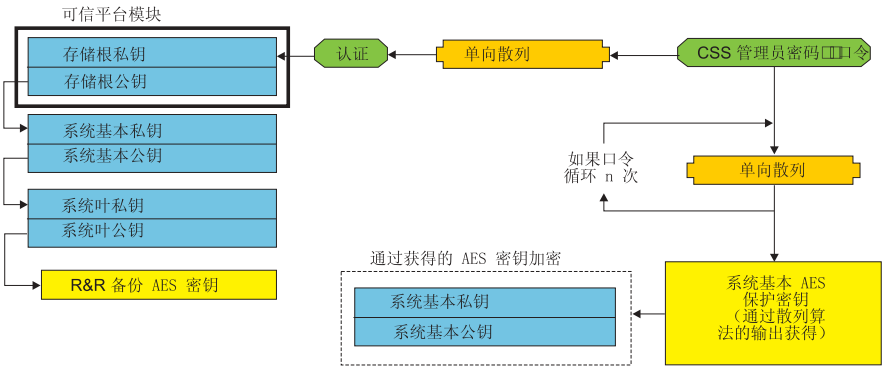

图 1.

为系统创建 SRK 后，可以在可信平台模块之外创建并存储其他密钥对，但由基于硬件的密钥对它们进行打包或保护。由于包含 SRK 的可信平台模块是硬件，而硬件可能受损，所以需要一种恢复机制以确保系统受损不会使数据恢复受阻。

为了恢复系统，将创建一个系统基本密钥（System Base Key）。这个可迁移的非对称存储密钥使客户端安全解决方案管理员能够从系统板交换恢复或从到另一个系统的计划迁移进行恢复。

为了保护系统基本密钥并允许在正常操作或恢复期间访问它，将创建该密钥的两个实例并使用两种不同的方法保护它们。首先，使用从已知客户端安全解决方案管理员的密码或客户端安全口令获得的 AES 对称密钥对系统基本密钥进行加密。客户端安全解决方案恢复密钥的这个副本仅用于从由于硬件故障而清除的可信平台模块或替换的系统板进行恢复。

客户端安全解决方案恢复密钥的第二个实例由 SRK 打包以将它导入密钥层次结构中。系统基本密钥的这个双实例使可信平台模块能够保护正常使用情况下绑定到它的机密，并允许通过系统基本密钥恢复发生故障的系统板（系统基本密钥使用客户端安全解决方案管理员密码或客户端安全口令解锁的 AES 密钥进行加密）。

然后创建系统叶密钥（System Leaf Key）。这个旧密钥是为保护系统级别的机密而创建的，如 Rescue and Recovery 用于保护备份的 AES 密钥。

登记用户

为了使同一个可信平台模块能够保护每个用户的数据，每个用户需要创建自己的用户基本密钥（User Base Key）。这个可迁移的非对称存储密钥也会创建两次并由根据每个用户的 Windows 密码或客户端安全口令生成的对称 AES 密钥保护。然后将用户基本密钥的第二个实例导入可信平台模块并由系统 SRK 提供保护。请参阅图 2。

用户级别密钥结构 — 登记用户

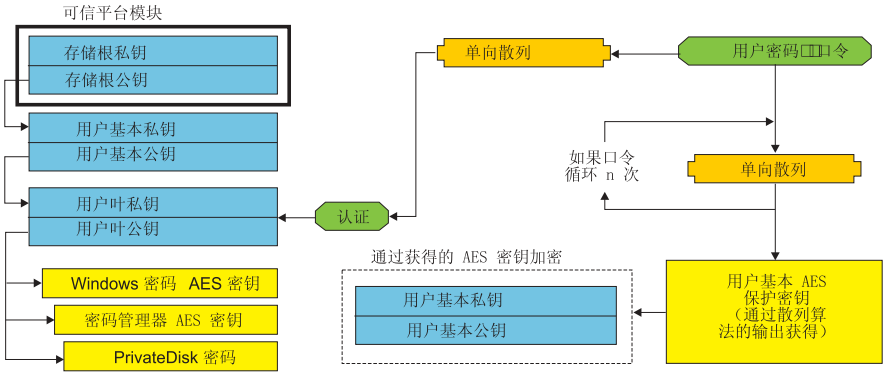

图 2.

创建用户基本密钥后，将创建第二个名为“用户叶密钥”的非对称密钥以保护个别机密，如用于保护因特网登录信息的密码管理器 AES 密钥、用于保护数据的 PrivateDisk 密码以及用于保护操作系统访问的 Windows 密码 AES 密钥。对用户叶密钥的访问由用户的 Windows 密码或客户端安全解决方案口令控制并且在登录期间自动解锁。

软件仿真

如果系统没有可信平台模块，将使用基于软件的信任根。用户可以获得相同的功能，但由于信任根是基于软件的密钥，所以安全性有所降低。可信平台模块的 SRK 将替换为基于软件的 RSA 密钥和 AES 密钥以提供可信平台模块提供的保护。RSA 密钥将 AES 密钥打包，而 AES 密钥则用于对层次结构中的下一个 RSA 密钥进行加密。

系统板交换

系统板交换意味着密钥绑定到的旧 SRK 不再有效并且需要另一个 SRK。如果通过 BIOS 清除可信平台模块，也可能发生这种情况。

客户端安全解决方案管理员必需将系统安全证书绑定到新的 SRK。需要通过从客户端安全解决方案管理员的授权安全证书获得的系统基本 AES 保护密钥对系统基本密钥进行解密。请参阅图 3。

注: 如果客户端安全解决方案管理员是一个域用户标识并且已在另一台机器上更改该用户标识的密码；为了对系统基本密钥进行解密以实现恢复，需要知道登录需要进行恢复的系统时最后使用的密码。例如，在客户端安全解决方案的部署期间将配置其管理员用户标识和密码，如果在另一台机器上更改该用户的密码，则部署期间设置的原始密码将成为恢复系统所需的权限。

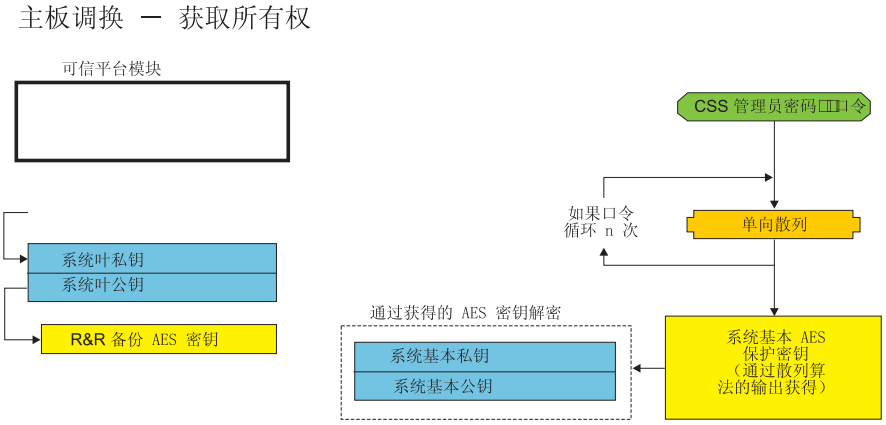

图 3.

按照以下步骤执行系统板交换:

1. 客户端安全解决方案管理员登录操作系统。
2. 登录执行代码（cssplanarswap.exe）将识别安全芯片已禁用并且需要重新引导才能启用。（可以通过在 BIOS 中启用安全芯片来避免这一步骤。）
3. 重新引导系统并启用安全芯片。
4. 客户端安全解决方案管理员登录；完成新的“获取所有权”过程。
5. 使用客户端安全解决方案管理员的认证获得的系统基本 AES 保护密钥对系统基本密钥进行解密。将系统基本密钥导入新的 SRK 中并重新建立系统叶密钥及其保护的所有安全证书。
6. 系统现已恢复完毕。

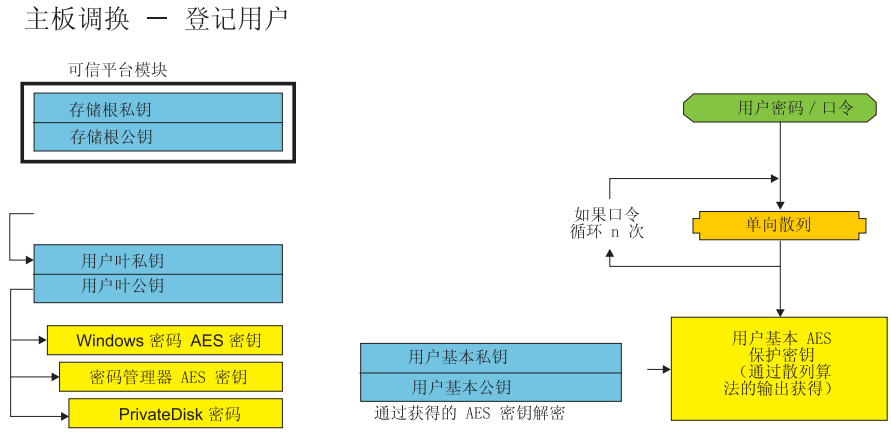

图 4.

当每个用户登录系统时，将自动通过从用户认证获得的用户基本 AES 保护密钥对用户基本密钥进行解密并将它导入通过客户端安全解决方案管理员创建的新 SRK 中。

XML 模式

xml 脚本编制旨在使 IT 管理员能够创建可用于部署客户端安全解决方案的定制脚本。脚本编制还提供客户端安全解决方案安装向导中提供的所有函数。xml_crypt_tool 可执行文件可以使用密码（AES 加密）或含糊内容保护脚本。创建脚本后，虚拟机（vmserver.exe）接受脚本作为输入。虚拟机调用与安装向导相同的函数对软件进行配置。

使用

所有脚本包含一个用于指定 xml 编码类型的标记（xml 模式）以及至少一个要执行的函数。该模式用于验证 xml 文件并检查所需的参数是否存在。目前不强制使用该模式。每个函数以函数标记括起。每个函数包含一个顺序，它指定了虚拟机执行命令的顺序（vmserver.exe）。每个函数还有一个版本号；目前所有函数都是 V1.0。为清晰起见，以下每个示例脚本都只包含一个函数。但是，实际使用时每个脚本很可能包含多个函数。客户端安全解决方案安装向导可用于创建此类脚本。请参阅第 137 页的『客户端安全向导』（有关详细信息，请参阅安装向导文档）。

注: 如果需要域名的任何函数缺少参数 <DOMAIN_NAME_PARAMETER>，将使用系统的缺省计算机名。

示例

AUTO_ENROLL_ADMIN_FOR_RNR_ONLY

该命令使系统管理员能够生成必要的安全密钥，使用 Rescue and Recovery 对备份进行加密时需要这些密钥。每个系统只应执行一次该命令；不应为每个用户执行该命令（仅限管理员）。

注: 如果只安装 Rescue and Recovery 并且要使用 TPM 对备份进行加密，则必须将管理员指定为 TPM 所有者。使用以下脚本文件自动指定管理员用户标识和密码。该 Windows 用户标识和密码将用于 TPM 恢复。（如果只安装 Rescue and Recovery，则所有其他 CSS XML 脚本函数都不适用。）

- **USER_NAME_PARAMETER**

  管理员用户的 Windows 用户标识。
- **DOMAIN_NAME_PARAMETER**

  管理员用户的域名。
- **RNR_ONLY_PASSWORD**

  管理员用户的 Windows 密码。

```
<?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

该命令启用可信平台模块并使用参数 SYSTEM_PAP。如果系统已设置 BIOS 管理员 / 超级用户密码，则必须提供该参数。否则，该参数是可选的。

```
<?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

该命令使用参数 SYSTEM_PAP。如果系统已设置 BIOS 管理员 / 超级用户密码，则必须提供该参数。否则，该参数是可选的。

```
<?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

使用 Rescue and Recovery 时，该命令启用通过客户端安全解决方案保护备份。

```
<?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

使用 Rescue and Recovery 来保护备份时，该命令禁用通过客户端安全解决方案保护备份。

```
<?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

该命令为所有客户端安全解决方案用户启用密码管理器。

```
 <?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

该命令启用客户端安全解决方案登录。

```
<?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

如果安装了 ThinkVantage Fingerprint Software，则该命令启用登录。

```
<?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

如果安装了 ThinkVantage Fingerprint Software，则该命令启用 “通过快速用户切换进行登录”（Logon with Fast User Switching）支持。

```
<?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

如果启用了 ThinkVantage Fingerprint Software 或客户端安全解决方案登录，则该命令禁用 ThinkVantage Fingerprint Software 和客户端安全解决方案登录。

```
<?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

该命令写入一个标志，客户端安全解决方案通过读取该标志来确定使用客户端安全口令还是 Windows 密码。

```
<?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

该命令启用在系统上使用 SafeGuard PrivateDisk。仍必须通过 ENABLE_PD_USER_FUNCTION 将每个用户特定地设置为使用 Safeguard PrivateDisk。

```
<?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

该命令写入一个标志，客户端安全解决方案通过读取该标志来确定客户端安全解决方案管理员用户的身份。参数为:

- **USER_NAME_PARAMETER**

  管理员用户的用户名。

- **DOMAIN_NAME_PARAMETER**

  管理员用户的域名。

```
<?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

该命令允许特定用户使用 PrivateDisk。参数为:

- **USER_NAME_PARAMETER**

  启用 PrivateDisk 的用户的用户名。

- **DOMAIN_NAME_PARAMETER**

  启用 PrivateDisk 的用户的域名。

- **PD_VOLUME_SIZE_PARAMETER**

  PrivateDisk 卷的大小（以兆字节为单位）。

- **PD_VOLUME_PATH_PARAMETER**

  要创建的 PrivateDisk 卷的路径。

- **PD_VOLUME_NAME_PARAMETER**

  要创建的 PrivateDisk 卷的名称。如果指定值 PD_USE_DEFAULT_OPTION，将自动使用缺省值。

- **PD_VOLUME_DRIVE_LETTER_PARAMETER**

  要创建的 PrivateDisk 卷的盘符。如果指定值 PD_USE_DEFAULT_OPTION，将自动使用缺省值。

- **PD_VOLUME_CERT_PARAMETER**

  如果传入值 PD_USE_CSS_CERT，则 PrivateDisk 将创建一个新证书或使用现有证书并使用客户端安全解决方案 CSP 保护它。该卷的安装／卸装将依赖于 CSP 而不是 CSS 口令／Windows 密码。如果指定值 PD_USE_DEFAULT_OPTION，则不使用证书并缺省使用用户的 CSS 口令／Windows 密码。

- **PD_USER_PASSWORD**

  客户端安全解决方案传递给 PrivateDisk 用于安装／创建 PrivateDisk 卷的密码。如果指定值 PD_RANDOM_VOLUME_PWD，则客户端安全解决方案将生成一个随机卷密码。

- **PD_VOLUME_USER_PASSWORD_PARAMETER**

  一个用于安装 PrivateDisk 卷的、特定于用户的密码。该密码将作为 PD_USER_PASSWORD 密码的备用密码。无论之后客户端安全解决方案因何种原因发生故障，传入该参数的值将独立于客户端安全解决方案。如果指定值 PD_USE_DEFAULT_OPTION，则不使用任何值。

```
<?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

该命令将系统初始化到系统中使用的客户端安全解决方案。通过这个函数调用生成所有系统范围的密钥。参数为:

- **NEW_OWNER_AUTH_DATA_PARAMETER**

  所有者密码初始化系统。如果未设置所有者密码，则传入该参数的值将成为新的所有者密码。如果已设置所有者口令并且管理员使用相同的密码，则可以将它传入。如果管理员要使用一个新的所有者口令，则应将所需的密码传入该参数。

- **CURRENT_OWNER_AUTH_DATA_PARAMETER**

  系统的当前所有者密码。如果系统已有 5.4x 所有者密码，则该参数应传入 5.4x 密码。否则，如果需要一个新的所有者密码，应将当前所有者密码传入该参数。如果不需要更改密码，则应传递值 NO_CURRENT_OWNER_AUTH。

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

该命令更改客户端安全解决方案管理员权限并对系统密钥做出相应的更新。通过这个函数调用重新生成所有系统范围的密钥。参数为:

- NEW_OWNER_AUTH_DATA_PARAMETER

  可信平台模块的新的所有者密码。

- CURRENT_OWNER_AUTH_DATA_PARAMETER

  可信平台模块的当前所有者密码。

```
<?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

该命令登记特定用户以使用客户端安全解决方案。该函数为给定用户创建所有特定于用户的安全密钥。参数为:

- **USER_NAME_PARAMETER**

  要登记的用户的用户名。

- **DOMAIN_NAME_PARAMETER**

  要登记的用户的域名。

- **USER_AUTH_DATA_PARAMETER**

  创建用户的安全密钥所使用的可信平台模块口令 / Windows 密码。

- **WIN_PW_PARAMETER**

  Windows 密码。

```
<?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

该命令设置特定可信平台模块用户的密码恢复。参数为:

- **USER_NAME_PARAMETER**

  要登记的用户的用户名。

- **DOMAIN_NAME_PARAMETER**

  要登记的用户的域名。

- **USER_PW_REC_QUESTION_COUNT**

  用户必须回答的问题数量。

- **USER_PW_REC_ANSWER_DATA_PARAMETER**

  特定问题的已存储答案。请注意，该参数的实际名称还带有一个数字，该数字对应于相应的问题。请参阅该命令的以下示例。

- **USER_PW_REC_STORED_PASSWORD_PARAMETER**

  用户正确回答所有问题后向该用户显示的已存储密码。

```
<?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

该命令写入一个标志，程序通过读取该标志来确定进入 Windows PE 环境时是否需要用户权限。参数为:

- **WIN_PE_LOGON_MODE_AUTH_PARAMETER**

  两个有效选项为:

  – 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>
```

第 5 章 系统迁移辅助程序定制

有两个可定制的系统迁移辅助程序部分:

- 编辑或修改命令文件
- 迁移其他应用程序设置

创建命令文件

SMA 在捕获阶段中读取命令文件的内容并将设置归档。本部分包含命令文件以及它们可以包含的语句的相关信息。

系统迁移辅助程序提供一个缺省命令文件（command.xml），您可以将它作为模板来创建定制命令文件。如果您将 SMA 安装在缺省位置，则该文件位于 D:\%RR%\migration\bin 目录中。

注: 系统迁移辅助程序 5.0 使用 XML 技术来描述它的命令文件命令。

请考虑有关 SMA 5.0 命令文件的以下几点:

- 命令文件遵循 XML V1.0 语法。命令文件区分大小写。
- 每个命令和参数节必须以 <TagName> 开头以 </TagName> 结尾，并且必须在这些标记之间描述其值。
- 语法错误可能导致运行 SMA 时遇到错误。如果 SMA 遇到错误，它将错误写入日志文件中并继续操作。根据错误的严重性，最终结果可能存在缺陷。

命令文件命令

下表包含命令文件中可以使用的命令的相关信息（有关文件迁移或注册表的命令除外）:

表 10.

命令	参数	参数值和示例

<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>
		要选择某个桌面设置，请将参数设置为“true”。否则，将参数设置为“false”或者不指定它。
		
		例如:
		
		`<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>
		要选择某个桌面设置，请将参数设置为“true”。否则，将参数设置为“false”或者不指定它。
		
		例如:
		
		`<Network>`
		`<computer_name>true<computer_name>`
		`<mapped_drives>false</mapped_drives>`
		`</Network>`

<Applications>	<Application>
	
	有关所有受支持的应用程序的列表，请参阅 *ThinkVantage System Migration Assistant User's Guide*。
		例如:
		
		`<Applications>`
		`<Application>Lotus Notes</Application>`
		`<Application>Microsoft Office</Application>`
		`<//Applications>`
		
		或
		
		`<Applications>`
		`<Application>$(all)</Applications>`

<Registries>	• <Registry> • <hive> • <keyname> • <value>	要捕获或应用注册表设置，请在命令文件中将 hive、keyname 和 value 指定为参数。

表 10. (续)

命令	参数	参数值和示例

<IncUsers>	<UserName>	要捕获所有用户概要文件，为所有用户设置 $(all) 或使用 * 作为通配符。否则，请分别指定用户。
		
		以下通配符可用。
		• * 用于可变长度的通配符
		• % 用于固定长度的通配符（1 字符）
		
		例如:
		`<IncUsers>`
		`<UserName>administrator</UserName>`
		`<UserName>domain\Jim</UserName>`
		`</IncUsers>`

<ExcUsers>	<UserName>	要从迁移过程中排除用户，请指定用户的域名和用户名。 以下通配符可用。 • * 用于可变长度的通配符 • % 用于固定长度的通配符（1 字符）

<Printers>	<Printer>
	
	<PrinterName>
		该控制语句适用于源计算机和目标计算机。
		
		要捕获所有打印机，将该参数设置为 *&(all)*。否则，请分别指定每台打印机。要只捕获缺省打印机，将该参数设置为 *&(DefaultPrinter)*。
		
		例如:
		`<Printers>`
		`  <Printer>&(all)</Printer>`
		`</Printers>`
		
		`<Printers>`
		`  <Printer>`
		`   <PrinterName>IBM 5589-L36</PrinterName>`
		`  </Printer>`
		`</Printers>`
		
		`<Printers>`
		`  <Printer>&(DefaultPrinter)</Printer>`
		`</Printers>`

表 10. (续)

命令	参数	参数值和示例
<MISC>	<bypass_registry>	要取消选择所有注册表设置，请设置为“true”。否则，设置为“false”或者不指定它。
	<overwrite existing files>	要覆盖现有文件，请设置为“true”。否则，设置为“false”或者不指定它。
	<log_file_location>	要指定 SMA 写入日志文件的目录，请输入一个标准目录名。您可以指定另一个系统上的共享目录。 如果不设置该参数，SMA 将日志文件写入 d:/InstDir/（其中 d 是硬盘驱动器的盘符，/InstDir/ 是安装 SMA 的目录）。
	<temp_file_location>	要指定 SMA 写入临时文件的目录，请输入一个标准目录名。您可以指定另一个系统上的共享目录。 如果不设置该参数，SMA 将临时文件写入 d:/InstDir/etc/data（其中 d 是硬盘驱动器的盘符，/InstDir/ 是安装 SMA 的目录）。
	<resolve_icon_links>	要只复制那些带有活动链接的图标，请设置为“true”。否则，将参数设置为“false”或者不指定它。

文件迁移命令

SMA 按照以下顺序处理文件迁移命令：首先执行文件包括命令，然后从包括文件执行文件排除命令。

SMA 将根据源计算机上文件和文件夹的原位置选择和取消选择文件。文件重定向语句存储在概要文件中并在应用阶段进行解释。

处理文件名和目录名时不区分大小写。

下表包含文件迁移命令的相关信息。所有文件迁移命令都是可选的。

表 11.

命令	参数	具体操作

<FilesAndFolders>	<run>	要捕获或应用文件迁移，请将参数设置为“true”。否则，将参数设置为“false”或者不指定它。
		
		例如:
		
		`<FilesAndFolders>`
		`<run>true</run>`
		`</FilesAndFolders>`

<Exclude_drives>	<Drive>	指定要从驱动器扫描中排除的盘符。
		
		例如:
		
		`<ExcludeDrives>`
		`<Drive>D</Drive>`
		`<Drive>E</Drive>`
		`</ExcludeDrive>`

表 11. (续)

命令	参数	具体操作
<Inclusions>	<IncDescriptions> <Description> <DateCompare> <Operand> <Date> <SizeCompare> <Operand> <Size> <Dest> <Operation> 其中 • <Description> 是标准文件名。您可以对文件名和文件夹名称使用通配符。 • <DateCompare> 是可选参数，它根据文件的创建日期来指定文件。 – <Operand> 是 NEWER 或 OLDER。 – <Date> 是基线日期（使用月／日／年格式）。 • <SizeCompare> 是可选参数，用于根据文件大小选择文件。 – <Operand> 是 LARGER 或 SMALLER。 – <Size> 是文件大小（以 MB 为单位）。 • <Dest> 是可选参数，它指定目标系统上写入文件的目标文件夹的名称。 • <Operation> 是可选参数，它指定如何处理文件路径。它可以指定为以下某项: – P 保留文件路径并在目标系统上从 <Dest> 参数指定的位置开始重新创建文件。 – R 除去文件路径并将文件直接放入 <Dest> 参数指定的位置。	在指定的目录中搜索所有匹配的文件。 例如: 示例 1 <IncDescription> <Description>c:\MyWorkFolder\ls</Description> </IncDescription> **注**: 要指定文件夹名称，请在描述结尾处添加 .\. 示例 2 <IncDescription> <Descriptin>C:\MyWorkFolder*.*</Decsription> <DateCompare> <Operand>NEWER</Operand> <Date>07/31/2005</Date> </DateCompare> </IncDescription> 示例 3 <IncDescription> <Description>C:\MyWorkFolder/*.*</Description> <SizeCompare> <Operand>SMALLER</Operand> <Size>200</Size> </SizeCompare> </IncDescription> 示例 4 <IncDescription> <Description>C:\MyWorkFolder*.*</Description> <Dest>D:\MyNewWorkFolder</Dest> <Operation><IncDescription>

表 11. (续)

命令	参数	具体操作
<Exclusions>	<ExDescriptions> <Description> <DateCompare> <Operand> <Date> <SizeCompare> <Operand> <Size> 其中 • <Description> 是标准文件或文件夹名称。其中文件名和文件夹名称都可以包含通配符。 • <DateCompare> 是可选命令，您可以根据文件的创建日期用它来选择文件。 – <Operand> 是 NEWER 或 OLDER。 – <Date> 是基线日期（使用月／日／年格式）。 • <SizeCompare> 是可选参数，用于根据文件大小选择文件。 – <Operand> 是 LARGER 或 SMALLER。 – <Size> 是文件大小（以 MB 为单位）。	取消选择指定目录中的所有匹配文件 例如: 示例 1 <ExDescription> <Description>C:\YourWorkFolder</Description> </ExDescription> 示例 2 <ExDescription> <Description>C:\YourWorkFolder</Description> <DateCompare> <Operand>OLDER</Operand> <Date>07/31/2005</Date> </DateCompare> </ExDescription> 示例 3 <ExDescription> <Description>C:\YourWorkFolder</Description> <SizeCompare> <Operand>LARGER</Operand> <Size>200</Size></SizeCompare> </ExDescription>

文件迁移命令的示例

本部分包含文件迁移命令的示例。这些示例说明了如何将文件包括和文件排除命令结合起来对文件选择进行优化。其中只显示命令文件的文件处理部分。

在捕获阶段中选择文件

本部分包含用于在捕获阶段中选择文件的三个代码示例。

示例 1

以下代码示例选择所有扩展名为 .doc（Microsoft Word 文档）的文件并将它们重新定位到 “d:\My Documents” 目录中。它随后排除 d:\No_Longer_Used 目录中的所有文件

```
<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>
```

示例 2

以下代码示例选择驱动器的内容，排除 d 盘根目录中的所有文件以及扩展名为 .tmp 的所有文件。

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

示例 3

以下代码示例选择 c 盘的所有内容，排除 %windir%（它指定 Windows 目录）下的所有文件。

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

示例 4

以下代码示例选择 %USERPROFILE% 文件夹（它是当前登录用户的用户概要文件路径）的所有内容，排除扩展名为 .dat 的所有文件和 “Local Settings” 子文件夹。

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

迁移其他应用程序设置

注：要创建定制应用程序文件，您必须全面了解应用程序（包括定制设置的存储位置）。缺省情况下，SMA 预配置为迁移多个应用程序的设置。有关 SMA 支持的应用程序的列表，请参阅 *System Migration Assistant User's Guide*。您还可以创建一个定制应用程序文件，用于迁移其他应用程序的设置。

该文件必须命名为 application.xml 或 application.smaapp 并放在 d:\%RR%\Migration\bin\Apps 中（其中 *Apps* 指定应用程序并且 d 是硬盘驱动器的盘符）。当同一应用程序的 application.smaapp 和 application.xml 定制应用程序文件同时存在时，application.smaapp 的优先级更高。

要支持新的应用程序，您可以复制现有的应用程序文件并做出必要的更改。例如，Microsoft_Access.xml 是现有的应用程序文件。

请考虑有关应用程序文件的以下几点:

- *application*.xml
  - 缺省情况下，安装系统迁移辅助程序时，只存在 application.xml。
  - 以 “<!-” 和 “->” 括起的 <tag> 将作为注释。例如:

```
<!--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-->
```

  - 必须在不同的节中描述各个命令。
  - 每个节以标记括起的命令开头，例如: <AppInfo> 或 <Install_Directories>。可以在节中输入一个或多个字段；每个字段必须各占一行。
  - 如果应用程序文件包含语法错误，SMA 将继续操作并将错误写入日志文件。

表 12 显示了应用程序文件的相关信息:

表 12.

节	命令	值	具体操作
<Applications>			
	<Family>	文本字符串。忽略前导空格；不要以引号括起文本字符串。	指定应用程序的非版本特定名称。以批处理方式运行 SMA 时，在命令文件的 applications 节中使用该字符串。 例如: `<Family>adobe Acrobat Reader</Family>`
	<SMA_Version>	数字值。	指定 SMA 版本号。 例如: `<SMA_Version>SMA 5.0</SMA_Version`
	<App>	*ShortName*，其中 ShortName 是应用程序的特定于版本的短名称。	指定一个或多个应用程序的特定于版本的短名称。 例如: `<APP>Acrobat_Reader_50</APP>`
<Application ShortName=*ShortName*>，其中 *ShortName* 是您在 “Applications” 节中指定的应用程序的短名称。			
	<Name>	文本字符串	指定应用程序的名称。
	<Version>	数字值	指定应用程序的版本。

	<Detects>
	<Detect>
		Root，*PathAndKey*	指定注册表键。SMA 通过搜索指定的注册表键来检测应用程序。
			例如:
			`<Detects>`
			`<Detect>`
			`<hive>HKLM</hive>`
			`<keyname>Software\Adobe\Acrobat Reader\5.0\</keyname>`
			`</Detect>`
			`</Detects>`

表 12. (续)

<table>
<tr><th>节</th><th>命令</th><th>值</th><th>具体操作</th></tr>
<tr><td colspan="4"><Install_Directories>

例如:

<pre>
<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>
</pre></td></tr>
<tr><td></td><td><OS></td><td>文本字符串</td><td>OS 指定操作系统，它可以是以下某个操作系统:
• WinXP
• Win2000
• WinNT
• Win98</td></tr>
<tr><td></td><td><Registry></td><td>hive 是 HKLM 或 HKCU。

keyname 是键名。

value 是可选命令，它指定迁移的注册表值。</td><td>按照安装目录在注册表中的显示情况指定它。</td></tr>
<tr><td colspan="4"><Files_From_Folders>

可选</td></tr>
</table>

表 12. (续)

节	命令	值	具体操作

	SMAVariable\Location[|File][/s]
	
	其中
	• SMAvariable 是以下某个变量，它们指定定制文件的位置:
	– %Windows Directory%（操作系统文件的位置）
	– %Install Directory%（应用程序的位置，如 Install_Directories 节中定义的那样）
	– %Appdata Directory%（Application Data 目录，它是用户概要文件目录的子目录）
	– %LocalAppdata Directory%（Local Settings 文件夹中的 Application Data 目录，它是用户概要文件目录的子目录）
	– %Cookies Directory%（Cookies 目录，它是用户概要文件目录的子目录）
	– %Favorites Directory%（Favorites 目录，它是用户概要文件目录的子目录）
	– %%Personal Directory%（Personal 目录，它是用户概要文件目录的子目录（My Documents）。Windows NT4 不能使用该环境变量。）
			指定要迁移的定制文件。
			
			例如:
			`<Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi</Files_And_Folders>`
			
			SMA 捕获 %AppData Directory%\Adobe\Acrobat\Whapi 文件夹中的文件。不包括子目录中的文件。
			`<Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi\ /s</Files_From_Folder>`
			
			SMA 捕获 %AppData Directory%\Adobe\Acrobat\Whapi 文件夹中的文件。包括子目录中的文件。
			`<Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi\*.*</Files_From_Folder>`
			
			SMA 捕获 %AppData Directory%\Adobe\Acrobat\Whapi 文件夹中的文件。不包括子目录中的文件。
			`<Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi\*.* /s</Files_From_Folder>`
			
			SMA 捕获 %AppData Directory%\Adobe\Acrobat\Whapi 文件夹中的文件。包括子目录中的文件。
			`<Files_From_Folder>%AppData Directory%\Adobe\Acrobat\Whapi</Files_From_Folder>`
			
			当 “Whapi” 后面没有 “\” 时，SMA 将 “Whapi” 作为文件而不是文件夹。

	• *Location* 指定一个标准文件或目录。文件名中可以使用通配符，但路径中不可以。如果指定目录，将复制所有文件。 • *[File]* 是可选参数，仅当 Location 指定目录并且 File 为要复制的文件时可以使用它。文件名中可以使用通配符，但路径中不可以。 • *[\s]* 是可选参数。如果使用 [/s]，将复制子目录中的所有文件。 • SMA5.0 用户可以使用 Windows 环境变量。启动 SMA 的用户的环境变量用作 Windows 环境变量的值。		
<Registries> 可选			

表 12. (续)

节	命令	值	具体操作

	hive 是 HKLM 或 HKCU。
	
	keyname 是键名。value 是可选命令，它指定迁移的注册表值。
			指定要迁移的注册表项。
			
			例如:
			
			`<Registries>`
			`<Registry>`
			`<hive>HKCU</hive>`
			`<keyname>Software\Adobe\Acrobat</keyname>`
			`<value></value>`
			`</Registry>`
			`</Registries>`

<Registry_Excludes> 可选			

	hive 是 HKLM 或 HKCU。
	
	keyname 是键名。value 是可选命令，它指定迁移的注册表值。
			指定要从选定的注册表项排除的注册表键和值。
			
			例如:
			
			`<Registry_Excludes>`
			`<Registry>`
			`<hive>HKCU</hive>`
			`<keyname>Software\Adobe\Acrobat Reader\5.0\AdobeViewer`
			`</keyname>`
			`<value>xRes</value>`
			`</Registry>`
			`</Registry_Excludes>`

<Files_Through_Registry>			

	<OS>
	
	指定操作系统并且是以下某个值:
	• WinXP
	• Win2000
	• WinNT
	• Win98
	
	<Registry> 指定注册表项并且格式为 hive、keyname 和 value，其中:
	• hive 是 HKLM 或 HKCU。
	• keyname 是键名。
	• value 是可选命令，它指定迁移的注册表值。File 是文件名。可以使用通配符。
	
	File 是文件名。可以使用通配符。
			指定要迁移的定制文件。
			
			例如:
			
			`<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> 通过“应用”在 <Registries> 处理之前执行批处理。
			
			例如:
			
			`<PreTargetBatchProcessing>`
			`<!CDATA[copy /y c:\temp\*.* c:\migration`
			`del c:\migration\*.mp3`
			`</PreTargetBatchProcessing>`

表 12. (续)

节	命令	值	具体操作
<TargetBatchProcessing>			
	<TargetBatchProcessing> <!CDAT[batch commands]] <TargetBatchProcessing>		<TargetBatchProcessing> 通过 “应用” 在 <Registries> 处理之后执行批处理。 例如: <TargetBatchProcessing> <!CDATA[copy /y c:\temp*.* c:\migration del c:\migration*.mp3 <TargetBatchProcessing>

创建应用程序文件

要确定必须为定制应用程序文件迁移哪些应用程序设置，您必须对应用程序进行仔细测试。

完成以下步骤以创建应用程序文件:

1. 使用 ASCII 文本编辑器打开一个现有的 application.XML 文件。如果您将 SMA 安装在缺省位置，则 application.XML 文件位于 d:\%RR%\Migration\bin\Apps 目录中（其中 d 是硬盘驱动器的盘符）。
2. 为要迁移的应用程序和应用程序设置修改这个 application.XML 文件。
3. 修改 <Applications> 节中的信息。
4. 修改 <Application Shortname=*Shortname*> 节中的 <Name> 和 <Verison> 命令。
5. 确定必须迁移的注册表键:
   a. 单击**开始 → 运行**。 “运行” 窗口打开。在**打开**字段中，输入 regedit 并单击**确定**。 “注册表编辑器” 窗口打开。
   b. 在左侧窗格中，展开 **HKEY_LOCAL_MACHINE** 节点。
   c. 展开 **Software** 节点。
   d. 展开特定于供应商的节点，如 **Adobe**。
   e. 继续浏览，直至找到应用程序的注册表键。在该示例中，注册表键是 SOFTWARE\Adobe\Acrobat Reader\6.0。
   f. 设置 Detect 字段的值。例如:

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

6. 修改 Install_Directories 节中的 Name 和 Version 命令。
7. 确定到应用程序的安装目录的路径。
   a. 在 “注册表编辑器” 窗口中，浏览到 HKLM\SOFTWARE\Adobe\Acrobat Reader\6.0\InstallPath 节点。
   b. 将相应的命令添加到应用程序文件的 Install_Directories 节中。例如:

```
<Install_Directory>
<OS>WinXP</OS>
<Registry>
<hive>HKLM</hive
```

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

注: 如果 HKLM\Software\Microsoft\Windows\CurrentVersion\AppPaths 目录中找不到特定于应用程序的目录，您必须在 HKLM\Software 树中的其他位置找到一个包含相应安装路径的目录。然后，使用 <Install_Directories> 节中的键。

8. 在 <Files_From Folders> 节中，指定要迁移的定制文件。
   a. 由于许多应用程序在缺省情况下都将文件保存在 Documents and Settings 子目录中，请检查 Application Data 目录中是否存在与该应用程序相关的目录。如果发现此类目录，您可以使用以下命令来迁移目录和文件:

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

      其中 Location\ 是标准文件或目录，而 [File] 是可选参数，仅当 Location\ 指定目录时可以使用它。在 Adobe Reader 示例中，定制文件位于 Preferences 目录中。
   b. 检查所有相关的目录中可能存储在其中的个人设置。
   c. 检查 Local Settings 目录。
9. 确定要迁移的注册表项。它们将位于 HKCU（HKEY_CURRENT_USER）中。在应用程序文件的 <Registries> 节中添加相应的命令。
10. 将 application.XML 文件保存到 d:\Program Files\ThinkVantage\SMA\Apps 目录中（其中 d 是硬盘驱动器的盘符）。
11. 测试新的应用程序文件。

Adobe Reader 的 application.XML 文件的示例

本部分包含 Adobe Reader 的一个应用程序文件。

```
<?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>
```

系统更新

Active Update

要确定是否已安装 Active Update Launcher，请检查以下注册表键是否存在:

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

要确定 Active Update Launcher 是否配置为允许 Active Update，TVT 检查自己的注册表键中 EnableActiveUpdate 属性的值。如果 EnableActiveUpdate=1，则 TVT 在 “帮助” 菜单下添加 ActiveUpdate 菜单项。

要调用 Active Update，调用 TVT 将启动 Active Update Launcher 程序并传递一个参数文件。

使用以下步骤来调用 Active Update:

1. 打开 Active Update Launcher 注册表键:

   ```
   HKLM\software\TVT\ActiveUpdate
   ```

2. 获取 Path 属性的值。
3. 获取 Program 属性的值。

第 6 章 安装

Rescue and Recovery／客户端安全解决方案安装程序包是将 InstallShield 10.5 Premier 作为 Basic MSI 项目开发的。InstallShield 10.5 Basic MSI 项目使用 Windows Installer 来安装应用程序，它为管理员提供了多项定制安装的功能（例如，从命令行设置属性值）。以下部分描述了使用和执行 Rescue and Recovery 3.0 安装程序包的方式。为了增进了解，请在阅读整个章节后再开始安装程序包。

注: 安装该程序包时，请参阅以下 Lenovo Web 页面中提供的自述文件:

www.Lenovo.com/ThinkVantage

该自述文件包含有关软件版本、受支持系统、系统需求以及其他注意事项等主题的最新信息以帮助您进行安装。

安装需求

本部分阐述安装 Rescue and Recovery／客户端安全解决方案程序包的系统需求。为得到最好的结果，请转至以下 Web 站点以确保您拥有最新版本的软件:

www.Lenovo.com/ThinkVantage

许多旧的 IBM 计算机在满足指定需求的前提下可以支持 Rescue and Recovery。有关支持 Rescue and Recovery 的 IBM 品牌的计算机的信息，请参阅 Web 上的下载页面。

IBM 和 Lenovo 品牌的计算机的需求

IBM 和 Lenovo 品牌的计算机必须满足或超出运行 Rescue and Recovery 的以下需求:

- 操作系统: Microsoft Windows XP 或 Windows 2000
- 处理器: Microsoft 指定用于 Windows XP（Home 或 Professional）和 Windows 2000 的处理器
  - 至少安装 service pack 1
- 内存: 128 MB
  - 在共享内存配置中，最大共享内存的 BIOS 设置必须设置为不小于 4 MB 且不大于 8 MB。
  - 在非共享内存配置中，非共享内存为 120 MB。

    注: 如果计算机的非共享内存小于 200 MB，则 Rescue and Recovery 仍能够运行。但是，用户在 Rescue and Recovery 环境中可能无法启动多个应用程序。
- 1.5 GB 可用硬盘空间（基本安装需要 930 MB 并且不包含 Rescue and Recovery 备份所需的空间）
- 支持 800 x 600 分辨率和 24 位真彩色的 VGA 兼容视频
- 受支持的以太网卡

非 IBM 或非 Lenovo 计算机上的安装和使用需求

在非 IBM 或非 Lenovo 计算机上进行安装具有以下需求:

安装需求

1.5 GB 可用硬盘空间。基本安装使用 930 MB 硬盘空间。

最小系统内存需求

非 IBM 或非 Lenovo 计算机必须具备 128 MB 系统 RAM 才能安装 Rescue and Recovery。

硬盘驱动器配置

原始设备制造商（OEM）计算机（非 IBM 或非 Lenovo）的“出厂预装入”不支持 Rescue and Recovery 程序。对于 OEM 计算机，硬盘驱动器必须根据第 107 页的『在非 IBM 品牌的计算机上安装 Rescue and Recovery』中的建议进行配置。

网络适配器

Rescue and Recovery 环境只支持已连线、基于 PCI 的以太网网络适配器。Rescue and Recovery 环境中包含的网络设备驱动程序与 Microsoft Windows XP Professional 操作系统中预填充的驱动程序相同，并且它们独立于 Windows 操作系统。对于受支持的 Lenovo 和 IBM 品牌的计算机，Rescue and Recovery 软件本身包含所需的驱动程序。

如果计算机中的 OEM 网络设备不受支持，请参阅该设备随附的文档以获取有关为特定于系统的网络驱动程序添加支持的说明。从您的 OEM 请求驱动程序。

支持从外部介质（CD/DVD 和 USB）引导

非 IBM／非 Lenovo 计算机和设备（USB 硬盘驱动器、CD-R/RW、DVD-R/RW/RAM 或 DVD+R/RW）必须完全支持以下一种或多种规格:

- ATAPI 可移动介质设备 BIOS 规格
- BIOS 增强磁盘驱动器服务 – 2
- Compaq Phoenix Intel® BIOS 引导规格
- El Torito 可引导 CD-ROM 格式规格
- USB 大容量存储类规格概述（每个设备必须符合命令块规格，该规格位于“USB 大容量存储类规格概述”中的 2.0 子类代码一节中。）
- 用于引导的 USB 大容量存储规格

视频需求

- **视频兼容性**: 支持 800 x 600 分辨率和 24 位真彩色的 VGA 兼容视频
- **显存**:
  - 在非共享显存系统上: 最小 4 MB 的视频 RAM
  - 在共享显存系统上: 最小 4 MB 最大 8 MB 可以分配给显存。

应用程序兼容性

某些具有复杂过滤驱动程序环境（如反病毒软件）的应用程序可能与 Rescue and Recovery 软件不兼容。有关兼容性问题的信息，请参阅以下 Web 站点上 Rescue and Recovery 软件随附的自述文件:

www.lenovo.com/ThinkVantage

实用程序

本指南涉及许多实用程序。这些实用程序可以在以下 Web 站点上找到:

www.Lenovo.com/ThinkVantage

Rescue and Recovery 的安装组件

1. 主安装程序包（约 45 MB）：这是根据安装项目源代码构建的 setup.exe。构建过程中会将 setup.exe 文件重命名为另一个名称，该名称表示了项目标识、介质类型、构建级别、国家或地区代码（该案例中始终为 US）以及补丁代码 – 如 Z096ZIS1001US00.exe。这是一个自解压安装程序包，它会解压缩安装源文件并使用 Windows Installer 启动安装。它包含安装逻辑和 Windows 应用程序文件。该程序包不包含任何 predesktop 文件。
2. Predesktop US 基本程序（约 135 MB）：这是受密码保护的 zip 文件，它包含整个 predesktop US 基本程序。该文件名称格式为 Z062ZAA1001US00.TVT（其中 *AA* 决定了 predesktop 的兼容性，而 *001* 是 predesktop 的级别）。该文件是在所有语言系统上安装 predesktop 必需的。它必须与主安装程序包（setup.exe 或 Rescue and Recovery/Client Security Solution.msi – 如果解压缩或 OEM 安装）位于同一目录中。例外情况有两种：如果已安装 predesktop 并且不需要对它进行升级，或是执行安装时在命令行设置了属性 PDA=0 并且尚未安装（任何版本的）predesktop。setup.exe 包含一个文件 pdaversion.txt，它包含可与 Windows 版本一起使用的 predesktop 的最低版本。setup.exe 安装程序将使用以下逻辑查找 predesktop 文件：
   - **存在旧版本的 Predesktop（RNR 1.0 或 2.X）或者不存在任何 Predesktop**：

     安装程序将使用兼容性代码（如 AA，AB）查找 .TVT 文件，该代码相当于最低版本兼容性代码以及一个大于或等于最低版本级别的代码（.TVT 文件名中的所有其他版本字段必须与最低版本完全匹配）。如果找不到满足这些条件的文件，则停止安装。
   - **存在新版本的 Predesktop（RNR 3.0）**：

     安装程序将当前 predesktop 的兼容性代码与最低版本兼容性代码进行比较，并根据结果执行以下操作：
     - **当前代码 > 最低代码**：

       安装程序会显示消息，表明当前环境与该版本的 RNR 不兼容。
     - **当前代码 = 最低代码**：

       安装程序将当前版本级别与最低版本级别进行比较。如果当前级别大于或等于最低级别，安装程序将使用兼容性代码（AA，AB...）查找 .TVT 文件，该代码相当于最低版本兼容性代码以及一个大于当前版本级别的级别（.TVT 文件名中的所有其他版本字段必须与最低版本完全匹配）。如果找不到文件，安装过程将继续但不会更新 predesktop。如果当前级别小于最低级别，安装程序将使用兼容性代码（AA，AB，...）查找 .TVT 文件，该代码相当于最低版本兼容性代码以及一个大于或等于最低版本级别的级别（.TVT 文件名中的所有其他版本字段必须与最低版本完全匹配）。如果找不到满足这些条件的文件，则停止安装。
     - **当前代码 < 最低代码**：

       安装程序将使用兼容性代码（AA，AB，...）查找 .TVT 文件，该代码相当于最低版本兼容性代码以及一个大于或等于最低版本级别的代码（.TVT 文件名中的所有其他版本字段必须与最低版本完全匹配）。如果找不到满足这些条件的文件，则停止安装。

3. Predesktop 语言包（每个约 5 - 30 MB）：Windows PE 有 24 个 Rescue and Recovery 3.0 中受支持的语言包。每个语言包以格式 Z062ZAA1001CC00.TVT 命名（其中 CC 表示语言）。如果将 predesktop 安装在非英语系统或使用非支持语言的系统中，则需要其中某个文件并且该文件必须与主安装程序包及 US predesktop .TVT 文件位于同一目录中。如果 Windows 为非英语版本或使用语言包不支持的语言，则语言包的语言必须与 Windows 使用的语言匹配。如果正在安装或更新 predesktop 并且需要语言包，安装将查找 .TVT 语言包（其中，文件名的所有字段与 US predesktop 文件名匹配，但语言代码除外，它必须与系统语言匹配）。语言包提供以下语言:
   - 阿拉伯语
   - 巴西葡萄牙语
   - 葡萄牙语
   - 捷克语
   - 丹麦语
   - 芬兰语
   - 法语
   - 希腊语
   - 德语
   - 希伯来语
   - 中文（香港特别行政区）
   - 匈牙利语
   - 意大利语
   - 日语
   - 韩国语
   - 荷兰语
   - 挪威语
   - 波兰语
   - 葡萄牙语
   - 俄语
   - 简体中文
   - 西班牙语
   - 瑞典语
   - 繁体中文
   - 土耳其语

标准安装过程和命令行参数

Setup.exe 可以接受一组命令行参数，如下所述。需要参数的命令行选项必须指定为选项及其参数之间无空格。例如，Setup.exe /s /v″/qn REBOOT=”R”″ 有效，而 Setup.exe /s /v ″/qn REBOOT=”R”″ 无效。仅当参数包含空格时，选项的参数两侧需要引号。

注: 单独执行安装（在不使用任何参数的情况下运行 setup.exe）时，它的缺省行为是在安装结束时提示用户重新引导。重新引导是确保程序能正确运行所必需的。如前文及示例部分所述，可以通过静默安装中的命令行参数来延迟重新引导。

以下参数和描述直接摘自 InstallShield 开发者帮助文档（InstallShield Developer Help Documentation）。其中已删除不适用于 Basic MSI 项目的参数。

表 13.

参数	描述
/a: 管理安装	/a 开关使 Setup.exe 执行管理安装。管理安装将您的数据文件复制（并解压缩）到用户指定的目录，但不创建快捷方式、注册 COM 服务器或创建卸载日志。
/x: 卸载方式	/x 开关使 Setup.exe 卸载先前安装的产品。
/s: 静默方式	命令 Setup.exe /s 禁止 Basic MSI 安装程序的 Setup.exe 初始化窗口，但不会读取响应文件。Basic MSI 项目不创建或使用静默安装的响应文件。要静默运行 Basic MSI 产品，请运行命令行 Setup.exe /s /v/qn。（要指定 Basic MSI 静默安装的公共属性的值，可以使用 Setup.exe /s /v″/qn INSTALLDIR=D:\Destination″ 等命令。）
/v: 将参数传递到 Msiexec	/v 参数用于将命令行开关和公共属性的值传递到 Msiexec.exe。
/L: 安装语言	用户可以使用带有十进制语言标识的 /L 开关指定多语言安装程序使用的语言。例如，指定德语的命令为 Setup.exe /L1031。注: 并非表 14 中提到的所有语言均受安装支持。
/w: 等待	对于 Basic MSI 项目，/w 参数强制 Setup.exe 等待，直至安装完成后才退出。如果在批处理文件中使用 /w 选项，您可能需要在整个 Setup.exe 命令行参数之前添加 start /WAIT。该用法的正确格式示例如下: `start /WAIT setup.exe /w`

表 14.

语言	标识
阿拉伯语（沙特阿拉伯）	1025
巴斯克语	1069
保加利亚语	1026
加泰罗尼亚语	1027
简体中文	2052
繁体中文	1028
克罗地亚语	1050
捷克语	1029
丹麦语	1030
荷兰语（标准）	1043
英语	1033
芬兰语	1035
法语加拿大语	3084
法语	1036

表 14. (续)

语言	标识
德语	1031
希腊语	1032
希伯来语	1037
匈牙利语	1038
印度尼西亚语	1057
意大利语	1040
日语	1041
韩国语	1042
挪威语（博克马尔语）	1044
波兰语	1045
葡萄牙语（巴西）	1046
葡萄牙语（标准）	2070
罗马尼亚语	1048
俄语	1049
斯洛伐克语	1051
斯洛文尼亚语	1060
西班牙语	1034
瑞典语	1053
泰语	1054
土耳其语	1055

管理安装过程和命令行参数

Windows Installer 可以针对网络执行应用程序或产品的管理安装以供工作组使用或用于定制。对于 Rescue and Recovery／客户端安全解决方案安装程序包，管理安装将安装源文件解压缩到指定的位置。要运行管理安装，需要使用 /a 参数从命令行执行安装程序包:

```
Setup.exe /a
```

启动管理安装会出现一系列对话框屏幕，提示管理用户指定安装文件的解压缩位置。向管理用户显示的缺省解压缩位置是 C:\。可以选择新的位置，该位置可能包含 C: 以外的驱动器（如其他本地驱动器和映射的网络驱动器）。也可以在该步骤中创建新目录。

如果静默运行管理安装，则可以在命令行设置公共属性 TARGETDIR 以指定解压缩位置:

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

完成管理安装后，管理用户可以定制源文件（例如，向 tvt.txt 添加附加设置）。要在定制后使用解压缩的源文件进行安装，用户需要从命令行调用 msiexec.exe，传递解压缩的 msi 文件的名称。

以下部分描述了可以与 msiexec 结合使用的可用命令行参数及其使用方法的示例。公共属性也可以在 msiexec 命令行调用中直接设置。

MsiExec.exe 命令行参数

MsiExec.exe 是 Windows Installer 的可执行程序，用于解释安装程序包并在目标系统上安装产品:

```
msiexec. /i "C:WindowsFolder/Profiles\UserName\Persona\MySetups\project name\
product configuration\release name\DiskImages\Disk1\product name.msi
```

下表提供 MsiExec.exe 命令行参数的详细描述。该表直接摘自 Windows Installer 上的 Microsoft 平台 SDK 文档。

表 15.

参数	描述
/i *package* 或 *product code*	使用该格式安装产品 Othello: `msiexec /i "C:\WindowsFolder\Profiles\ UserName\Personal\MySetups\Othello\Trial Version\ Release\DiskImages\Disk1\Othello Beta.msi"` Product Code 指在产品项目视图的 Product Code 属性中自动生成的 GUID。
/f [p|o|e|d|c|a|u|m|s|v] *package* 或 *product code*	安装时带有 /f 选项将修复或重新安装丢失的或毁坏的文件。 例如，要强制重新安装所有文件，请使用以下语法: `msiexec /fa "C:\WindowsFolder\Profiles\ UserName\Personal\MySetups\Othello\Trial Version\ Release\DiskImages\Disk1\Othello Beta.msi"` 可以结合以下标志: • p 如果缺少文件，则重新安装该文件 • o 如果缺少文件或用户系统上存在文件的较早版本，则重新安装该文件 • e 如果缺少文件或用户系统上存在文件的等同或较早版本，则重新安装该文件 • c 如果缺少文件或已安装文件的存储校验和与新文件的值不匹配，则重新安装该文件 • a 强制重新安装所有文件 • u 或 m 重写所有必需的用户注册表项 • s 覆盖任何现有的快捷方式 • v 从源文件运行应用程序并重新高速缓存本地安装程序包
/a *package*	/a 选项允许具备管理员权限的用户将产品安装到网络上。
/x *package* 或 *product code*	/x 选项卸载产品。

表 15. (续)

参数	描述
/L [i|w|e|a|r|u|c|m|p|v|+] *log file*	使用 /L 选项进行构建会指定到日志文件的路径 – 这些标志表明要记录到日志文件中的信息: • i 记录状态消息 • w 记录非致命警告消息 • e 记录任何错误消息 • a 记录操作序列的起始 • r 记录特定于操作的记录 • u 记录用户请求 • c 记录初始用户界面参数 • m 记录内存不足消息 • p 记录终端设置 • v 记录详细输出设置 • + 追加到现有文件 • * 是通配符，它允许您记录所有信息（详细输出设置除外）
/q [n|b|r|f]	/q 选项用于结合以下标志设置用户界面级别: • q 或 qn 不创建用户界面 • qb 创建基本用户界面 以下的用户界面设置在安装结束时显示模态对话框: • qr 显示精简的用户界面 • qf 显示完整的用户界面 • qn+ 不显示用户界面 • qb+ 显示基本用户界面
/? 或 /h	两个命令都显示 Windows Installer 版权信息
TRANSFORMS	使用 TRANSFORMS 命令行参数指定要应用于基础包的任何转换。转换命令行调用可能类似于以下情况: `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"` 可以使用分号分隔多个转换。因此，建议您不要在转换名称中使用分号，因为 Windows Installer 服务无法对它们做出正确的解释。
属性	所有公共属性都可以从命令行进行设置或修改。公共属性是全部大写的，以示与专用属性的区别。例如，COMPANYNAME 是公共属性。 要从命令行设置属性，请使用以下语法: PROPERTY=VALUE。如果要更改 COMPANYNAME 的值，则应输入: `msiexec /i "C:\WindowsFolder\Profiles\UserName\Personal\MySetups\Your Project Name\Trial Version\My Release-1\DiskImages\Disk1\ProductName.msi" COMPANYNAME="InstallShield"`

标准 Windows Installer 公共属性

Windows Installer 有一组标准的内建公共属性，可以在命令行上设置它们以指定安装期间的特定行为。以下描述了命令行中最常用的公共属性。以下 Microsoft Web 站点提供更多文档：

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/about_properties.asp

表 16 显示了常用的 Windows Installer 属性：

表 16.

属性	描述
TARGETDIR	指定安装的根目标目录。在管理安装期间，该属性是复制安装程序包的位置。
ARPAUTHORIZEDCDFPREFIX	应用程序的更新通道的 URL。
ARPCOMMENTS	为“控制面板”上的“添加或删除程序”提供注释。
ARPCONTACT	为“控制面板”上的“添加或删除程序”提供联系。
ARPINSTALLLOCATION	到应用程序的主文件夹的标准路径。
ARPNOMODIFY	禁用修改产品的功能。
ARPNOREMOVE	禁用删除产品的功能。
ARPNOREPAIR	禁用程序向导中的“修复”按钮。
ARPPRODUCTICON	指定安装程序包的主图标。
ARPREADME	为“控制面板”上的“添加或删除程序”提供自述文件。
ARPSIZE	应用程序的估计大小（以千字节为单位）。
ARPSYSTEMCOMPONENT	阻止在“添加或删除程序”列表中显示应用程序。
ARPURLINFOABOUT	应用程序的主页的 URL。
ARPURLUPDATEINFO	应用程序更新信息的 URL。
REBOOT	REBOOT 属性禁止某些重新引导系统的提示。管理员通常在同时安装多个产品的一系列安装中使用该属性，这样只需在最后执行一次重新引导即可。设置 REBOOT=”R” 以禁用安装结束时的任何重新引导。
INSTALLDIR	该属性包含功能部件和组件的文件的缺省目标文件夹。

Rescue and Recovery 定制公共属性

Rescue and Recovery 程序的安装程序包包含一组定制公共属性，运行安装时可以在命令行上设置它们。可用的定制公共属性为：

表 17.

属性	描述
PDA	指定是否安装 predesktop，缺省值为 1。1 = 安装 predesktop，0 = 不安装 predesktop。注：如果已存在任何版本的 predesktop，则不使用该设置。
CIMPROVIDER	指定是否安装 CIM Provider 组件。缺省值为不安装该组件。在命令行上指定 CIMPROIVIDER=1 以安装该组件。
EMULATIONMODE	指定即使 TPM 存在，仍强制以仿真方式进行安装。在命令行上设置 EMULATIONMODE=1 以仿真方式进行安装。
HALTIFCSS54X	如果已安装 CSS 5.4X 并以静默方式运行安装，缺省值是以仿真方式继续安装。如果已安装 CSS 5.4X，则以静默方式运行安装时，使用 HALTIFCSS54X=1 属性停止安装。
HALTIFTPMDISABLED	如果 TPM 处于禁用状态并以静默方式运行安装，缺省值是以仿真方式继续安装。如果已禁用 TPM，则以静默方式运行安装时，使用 HALTIFTPMDISABLED=1 属性停止安装。
ENABLETPM	在命令行上设置 ENABLETPM=0 以防止安装启用 TPM。
NOCSS	在命令行上设置 NOCSS=1 以防止安装客户端安全解决方案及其子功能部件。该属性是为静默安装提供的，但也能用于 UI 安装。在 UI 安装中，定制安装屏幕中不会显示 CSS 功能部件。
NOPRVDISK	在命令行上设置 NOPRVDISK=1 以防止安装 SafeGuard PrivateDisk 功能部件。该属性是为静默安装提供的，但也能用于 UI 安装。在 UI 安装中，定制安装屏幕中不会显示 SafeGuard PrivateDisk 功能部件。
NOPWMANAGER	在命令行上设置 NOPWMANAGER=1 以防止安装密码管理器功能部件。该属性是为静默安装提供的，但也能用于 UI 安装。在 UI 安装中，定制安装屏幕中不会显示密码管理器功能部件。
NOCSSWIZARD	在命令行上设置 NOCSSWIZARD=1 以防止未登记的管理员用户登录时显示 CSS 向导。该属性是为要安装 CSS、但稍后使用脚本编制对系统进行实际配置的人员提供的。
CSS_CONFIG_SCRIPT	设置 CSS_CONFIG_SCRIPT="*filename*" 或 "*filename password*"，在用户完成安装和重新引导后运行配置文件。

表 17. (续)

属性	描述
SUPERVISORPW	在命令行上设置 SUPERVISORPW=”*password*” 以提供超级用户密码，从而在静默安装或非静默安装方式中启用芯片。如果已禁用芯片并以静默方式运行安装，则必须提供正确的超级用户密码以启用芯片，否则无法启用芯片。

安装日志文件

如果以 setup.exe 启动安装（通过双击主安装执行文件，无需使用参数即可运行主执行文件；或者，解压缩 msi 并执行 setup.exe），将在 %temp% 目录中创建一个日志文件 rrinstall30.log。该文件包含可用于调试安装问题的日志消息。直接从 msi 程序包运行安装时不会创建该日志文件；这包括从 “添加/删除程序” 执行的任何操作。要为所有 MSI 操作创建一个日志文件，您可以启用注册表中的记录策略。要这样做，请创建以下值:

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

安装示例

下表显示了使用 setup.exe 的示例:

表 18.

描述	示例
不带重新引导的静默安装	`setup.exe /s /v"/qn REBOOT="R""`
管理安装	`setup.exe /a`
指定解压缩位置的静默管理安装	`setup.exe /a /s /v"/qn TARGETDIR="F:\TVTRR""`
静默卸载	`setup.exe /s /x /v/qn`
不带重新引导的安装并在 temp 目录中创建安装日志	`setup.exe /v"REBOOT="R" /L*v %temp%\rrinstall30.log"`
安装（但不安装 predesktop）	`setup.exe /vPDA=0`

下表显示了使用 Rescue and Recovery/Client Security Solution.msi 的安装示例:

表 19.

描述	示例
安装	msiexec /i “C:\TVTRR\Rescue and Recovery/Client Security Solution.msi”
不带重新引导的静默安装	msiexec /i “C:\TVTRR\Rescue and Recovery/Client Security Solution.msi” /qn REBOOT=”R”
静默卸载	msiexec /x “C:\TVTRR\Rescue and Recovery/Client Security Solution.msi” /qn
安装（但不安装 predesktop）	msiexec /i “C:\TVTRR\Rescue and Recovery/Client Security Solution.msi” PDA=0

在磁盘映像中包含 Rescue and Recovery

您可以使用所选工具来创建包含 Rescue and Recovery 的磁盘映像。该部署指南提供有关 PowerQuest 和 Ghost 应用于该应用程序和安装的基本信息。假定您具备使用映像创建工具的技能并且将包含应用程序所需的其他选项。

注: 如果您计划创建映像，则必须捕获主引导记录。主引导记录对于 Rescue and Recovery 环境的正确运行十分关键。

使用基于 PowerQuest 驱动器映像的工具

假定 PowerQuest DeployCenter 工具 PQIMGCTR 安装在位置 X:\PQ，您可以使用带有以下脚本的 Rescue and Recovery 创建并部署映像:

最小脚本文件

表 20. X:\PQ\RRUSAVE.TXT

脚本语言	结果
SELECT DRIVE 1	选择第一硬盘驱动器
SELECT PARTITION ALL （当您的映像中有 12 型分区或多个分区时需要。）	选择全部分区
Store with compression high	存储映像

表 21. X:\PQ\RRDEPLY.TXT

脚本语言	结果
SELECT DRIVE 1	选择第一硬盘驱动器
DELETE ALL	删除全部分区
SELECT FREESPACE FIRST	选择第一可用空间
SELECT IMAGE ALL	选择映像中的全部分区
RESTORE	复原映像

映像创建

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

脚本语言	结果
SELECT DRIVE 1	选择第一硬盘驱动器
X:\PQ\PQIMGCTR	映像程序
/CMD=X:\PQ\RRUSAVE.TXT	PowerQuest 脚本文件
/MBI=1	捕获 Rescue and Recovery 引导管理器
/IMG=X:\IMAGE.PQI	映像文件

映像部署

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

脚本语言	结果
SELECT DRIVE 1	选择第一硬盘驱动器

表 23. X:\PQ\PQIMGCTR / CMD=X:\PQ\RRDEPLY.TXT /MBI=1 / IMG=X:\IMAGE.PQI (续)

脚本语言	结果
X:\PQ\PQIMGCTR	映像程序
/CMD=X:\PQ\RRDEPLY.TXT	PowerQuest 脚本文件
/MBR=1	复原 Rescue and Recovery 引导管理器
/IMG=X:\IMAGE.PQI	映像文件

使用基于 Symantec Ghost 的工具

创建 Ghost 映像时，必须使用命令行开关（可以合并到 GHOST.INI 文件中）-ib 以捕获 Rescue and Recovery 引导管理器。并且，映像必须捕获整个磁盘和所有分区。有关 Ghost 的特定详细信息，请参阅 Symantec 提供的文档。

客户端安全解决方案 V6.0 的安装组件

客户端安全解决方案 6.0 安装程序包是将 InstallShield 10.5 Premier 作为 Basic MSI 项目开发的。InstallShield 10.5 Basic MSI 项目使用 Windows Installer 来安装应用程序，它为管理员提供了多项定制安装的功能（例如，从命令行设置属性值）。以下部分描述了使用和执行 CSS 6.0 安装程序包的方式。为了增进了解，请阅读以下所有说明。

安装组件

CSS 6.0 安装只包含一个可执行文件（约 20 MB）。这是根据安装项目源代码构建的 setup.exe。构建过程中会将 setup.exe 文件重命名为另一个名称，该名称表示了项目标识、介质类型、构建级别、国家或地区代码（该案例中始终为 US）以及补丁代码 – 如 169ZIS1001US00.exe。这是一个自解压安装程序包，它会解压缩安装源文件并使用 Windows Installer 启动安装。它包含安装逻辑和 Windows 应用程序文件。

标准安装过程和命令行参数

Setup.exe 可以接受一组命令行参数，如下所述。需要参数的命令行选项必须指定为选项及其参数之间无空格。例如，

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

有效，而

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

无效。仅当参数包含空格时，选项的参数两侧需要引号。

注: 单独执行安装（在不使用任何参数的情况下运行 setup.exe）时，它的缺省行为是在安装结束时提示用户重新引导。重新引导是确保程序能正确运行所必需的。如前文及示例部分所述，可以通过静默安装中的命令行参数来延迟重新引导。

以下参数和描述直接摘自 InstallShield 开发者帮助文档（InstallShield Developer Help Documentation）。其中已删除不适用于 Basic MSI 项目的参数。

表 24.

参数	描述
/a: 管理安装	/a 开关使 Setup.exe 执行管理安装。管理安装将您的数据文件复制（并解压缩）到用户指定的目录，但不创建快捷方式、注册 COM 服务器或创建卸载日志。
/x: 卸载方式	/x 开关使 Setup.exe 卸载先前安装的产品。
/s: 静默方式	命令 Setup.exe /s 禁止 Basic MSI 安装程序的 Setup.exe 初始化窗口，但不会读取响应文件。Basic MSI 项目不创建或使用静默安装的响应文件。要静默运行 Basic MSI 产品，请运行命令行 Setup.exe /s /v/qn。（要指定 Basic MSI 静默安装的公共属性的值，可以使用 Setup.exe /s /v″/qn INSTALLDIR=D:\Destination″ 等命令。）
/v: 将参数传递到 Msiexec	/v 参数用于将命令行开关和公共属性的值传递到 Msiexec.exe。
/L: 安装语言	用户可以使用带有十进制语言标识的 /L 开关指定多语言安装程序使用的语言。例如，指定德语的命令为 Setup.exe /L1031。注: 并非表 25 中提到的所有语言均受安装支持。
/w: 等待	对于 Basic MSI 项目，/w 参数强制 Setup.exe 等待，直至安装完成后才退出。如果在批处理文件中使用 /w 选项，您可能需要在整个 Setup.exe 命令行参数之前添加 start /WAIT。该用法的正确格式示例如下: `start /WAIT setup.exe /w`

表 25.

语言	标识
阿拉伯语（沙特阿拉伯）	1025
巴斯克语	1069
保加利亚语	1026
加泰罗尼亚语	1027
简体中文	2052
繁体中文	1028
克罗地亚语	1050
捷克语	1029
丹麦语	1030
荷兰语（标准）	1043
英语	1033
芬兰语	1035
法语加拿大语	3084
法语	1036
德语	1031
希腊语	1032

表 25. (续)

语言	标识
希伯来语	1037
匈牙利语	1038
印度尼西亚语	1057
意大利语	1040
日语	1041
韩国语	1042
挪威语（博克马尔语）	1044
波兰语	1045
葡萄牙语（巴西）	1046
葡萄牙语（标准）	2070
罗马尼亚语	1048
俄语	1049
斯洛伐克语	1051
斯洛文尼亚语	1060
西班牙语	1034
瑞典语	1053
泰语	1054
土耳其语	1055

管理安装过程和命令行参数

Windows Installer 可以针对网络执行应用程序或产品的管理安装以供工作组使用或用于定制。对于 Rescue and Recovery／客户端安全解决方案安装程序包，管理安装将安装源文件解压缩到指定的位置。要运行管理安装，需要使用 /a 参数从命令行执行安装程序包:

```
Setup.exe /a
```

启动管理安装会出现一系列对话框屏幕，提示管理用户指定安装文件的解压缩位置。向管理用户显示的缺省解压缩位置是 C:\。可以选择新的位置，该位置可能包含 C: 以外的驱动器（如其他本地驱动器和映射的网络驱动器）。也可以在该步骤中创建新目录。

如果静默运行管理安装，则可以在命令行设置公共属性 TARGETDIR 以指定解压缩位置:

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

完成管理安装后，管理用户可以定制源文件（例如，向 tvt.txt 添加附加设置）。要在定制后使用解压缩的源文件进行安装，用户需要从命令行调用 msiexec.exe，传递解压缩的 msi 文件的名称。以下部分描述了可以与 msiexec 结合使用的可用命令行参数及其使用方法的示例。公共属性也可以在 msiexec 命令行调用中直接设置。

MsiExec.exe 命令行参数

MsiExec.exe 是 Windows Installer 的可执行程序，用于解释安装程序包并在目标系统上安装产品:

```
msiexec. /i "C:WindowsFolder/Profiles\UserName\Persona\MySetups\project name
  \product configuration\release name\DiskImages\Disk1\product name.msi
```

下表提供 MsiExec.exe 命令行参数的详细描述。该表直接摘自 Windows Installer 上的 Microsoft 平台 SDK 文档。

表 26.

参数	描述
/i *package* 或 *product code*	使用该格式安装产品 Othello: `msiexec /i "C:\WindowsFolder\Profiles\UserName\ Personal\MySetups\Othello\Trial Version\Release \DiskImages\Disk1\Othello Beta.msi"` Product Code 指在产品项目视图的 Product Code 属性中自动生成的 GUID。
f [p|o|e|d|c|a|u|m|s|v] *package* 或 *product code*	安装时带有 /f 选项将修复或重新安装丢失的或毁坏的文件。 例如，要强制重新安装所有文件，请使用以下语法: `msiexec /fa "C:\WindowsFolder\Profiles\UserName\ Personal\MySetups\Othello\Trial Version\Release \DiskImages\Disk1\Othello Beta.msi"` 可以结合以下标志: • p 如果缺少文件，则重新安装该文件 • o 如果缺少文件或用户系统上存在文件的较早版本，则重新安装该文件 • e 如果缺少文件或用户系统上存在文件的等同或较早版本，则重新安装该文件 • c 如果缺少文件或已安装文件的存储校验和与新文件的值不匹配，则重新安装该文件 • a 强制重新安装所有文件 • u 或 m 重写所有必需的用户注册表项 • s 覆盖任何现有的快捷方式 • v 从源文件运行应用程序并重新高速缓存本地安装程序包
/a *package*	/a 选项允许具备管理员权限的用户将产品安装到网络上。
/x *package* 或 *product code*	/x 选项卸载产品。

表 26. (续)

参数	描述
/L [i|w|e|a|r|u|c|m|p|v|+] *log file*	使用 /L 选项进行构建会指定到日志文件的路径 – 这些标志表明要记录到日志文件中的信息: • i 记录状态消息 • w 记录非致命警告消息 • e 记录任何错误消息 • a 记录操作序列的起始 • r 记录特定于操作的记录 • u 记录用户请求 • c 记录初始用户界面参数 • m 记录内存不足消息 • p 记录终端设置 • v 记录详细输出设置 • + 追加到现有文件 • * 是通配符，它允许您记录所有信息（详细输出设置除外）
/q [n|b|r|f]	/q 选项用于结合以下标志设置用户界面级别: • q 或 qn 不创建用户界面 • qb 创建基本用户界面 以下的用户界面设置在安装结束时显示模态对话框: • qr 显示精简的用户界面 • qf 显示完整的用户界面 • qn+ 不显示用户界面 • qb+ 显示基本用户界面
/? 或 /h	两个命令都显示 Windows Installer 版权信息
TRANSFORMS	使用 TRANSFORMS 命令行参数指定要应用于基础包的任何转换。转换命令行调用可能类似于以下情况: `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"` 可以使用分号分隔多个转换。因此，建议您不要在转换名称中使用分号，因为 Windows Installer 服务无法对它们做出正确的解释。
属性	所有公共属性都可以从命令行进行设置或修改。公共属性是全部大写的，以示与专用属性的区别。例如，COMPANYNAME 是公共属性。 要从命令行设置属性，请使用以下语法: PROPERTY=VALUE。如果要更改 COMPANYNAME 的值，则应输入: `msiexec /i "C:\WindowsFolder\Profiles\UserName \Personal\MySetups\Your Project Name\Trial Version\My Release-1\DiskImages\Disk1\ProductName.msi" COMPANYNAME="InstallShield"`

标准 Windows Installer 公共属性

Windows Installer 有一组标准的内建公共属性，可以在命令行上设置它们以指定安装期间的特定行为。以下描述了命令行中最常用的公共属性。以下 Microsoft 的 Web 站点提供更多文档：
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/about_properties.asp

表 27 显示了常用的 Windows Installer 属性：

表 27.

属性	描述
TARGETDIR	指定安装的根目标目录。在管理安装期间，该属性是复制安装程序包的位置。
ARPAUTHORIZEDCDFPREFIX	应用程序的更新通道的 URL。
ARPCOMMENTS	为“控制面板”上的“添加或删除程序”提供注释。
ARPCONTACT	为“控制面板”上的“添加或删除程序”提供联系。
ARPINSTALLLOCATION	到应用程序的主文件夹的标准路径。
ARPNOMODIFY	禁用修改产品的功能。
ARPNOREMOVE	禁用删除产品的功能。
ARPNOREPAIR	禁用程序向导中的“修复”按钮。
ARPPRODUCTICON	指定安装程序包的主图标。
ARPREADME	为“控制面板”上的“添加或删除程序”提供自述文件。
ARPSIZE	应用程序的估计大小（以千字节为单位）。
ARPSYSTEMCOMPONENT	阻止在“添加或删除程序”列表中显示应用程序。
ARPURLINFOABOUT	应用程序的主页的 URL。
ARPURLUPDATEINFO	应用程序更新信息的 URL。
REBOOT	REBOOT 属性禁止某些重新引导系统的提示。管理员通常在同时安装多个产品的一系列安装中使用该属性，这样只需在最后执行一次重新引导即可。设置 REBOOT=”R” 以禁用安装结束时的任何重新引导。
INSTALLDIR	该属性包含功能部件和组件的文件的缺省目标文件夹。

客户端安全解决方案定制公共属性

客户端安全解决方案程序的安装程序包包含一组定制公共属性，运行安装时可以在命令行上设置它们。可用的定制公共属性为：

表 28.

属性	描述
EMULATIONMODE	指定即使 TPM 存在，仍强制以仿真方式进行安装。在命令行上设置 EMULATIONMODE=1 以仿真方式进行安装。

表 28. (续)

属性	描述
HALTIFTPMDISABLED	如果 TPM 处于禁用状态并以静默方式运行安装，缺省值是以仿真方式继续安装。如果已禁用 TPM，则以静默方式运行安装时，使用 HALTIFTPMDISABLED=1 属性停止安装。
ENABLETPM	在命令行上设置 ENABLETPM=0 以防止安装启用 TPM。
NOPRVDISK	在命令行上设置 NOPRVDISK=1 以防止安装 SafeGuard PrivateDisk 功能部件。该属性是为静默安装提供的，但也能用于 UI 安装。在 UI 安装中，定制安装屏幕中不会显示 SafeGuard PrivateDisk 功能部件。
NOPWMANAGER	在命令行上设置 NOPWMANAGER=1 以防止安装密码管理器功能部件。该属性是为静默安装提供的，但也能用于 UI 安装。在 UI 安装中，定制安装屏幕中不会显示密码管理器功能部件。
NOCSSWIZARD	在命令行上设置 NOCSSWIZARD=1 以防止未登记的管理员用户登录时显示 CSS 向导。该属性是为要安装 CSS、但稍后使用脚本编制对系统进行实际配置的人员提供的。
CSS_CONFIG_SCRIPT	设置 CSS_CONFIG_SCRIPT="*filename*" 或 "*filename password*"，在用户完成安装和重新引导后运行配置文件。
SUPERVISORPW	在命令行上设置 SUPERVISORPW="*password*" 以提供超级用户密码，从而在静默安装或非静默安装方式中启用芯片。如果已禁用芯片并以静默方式运行安装，则必须提供正确的超级用户密码以启用芯片，否则无法启用芯片。

安装日志文件

如果以 setup.exe 启动安装（通过双击主安装执行文件，无需使用参数即可运行主执行文件；或者，解压缩 msi 并执行 setup.exe），将在 %temp% 目录中创建一个日志文件 cssinstall60.log。该文件包含可用于调试安装问题的日志消息。直接从 msi 程序包运行安装时不会创建该日志文件，这包括从 "添加/删除程序" 执行的任何操作。要为所有 MSI 操作创建一个日志文件，您可以启用注册表中的记录策略。要这样做，请创建以下值:

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

安装示例

下表显示了使用 setup.exe 的示例:

表 29.

描述	示例
不带重新引导的静默安装	`setup.exe /s /v"/qn REBOOT="R""`

表 29. (续)

描述	示例
管理安装	`setup.exe /a`
指定解压缩位置的静默管理安装	`setup.exe /a /s /v"/qn TARGETDIR="F:\CSS60""`
静默卸载	`setup.exe /s /x /v/qn`
不带重新引导的安装并在 temp 目录中创建安装日志	`setup.exe /v"REBOOT="R" /L*v %temp%\cssinstall60.log"`
安装（但不安装 predesktop）	`setup.exe /vPDA=0`

下表显示了使用 Client Security Solution.msi 的安装示例:

表 30.

描述	示例
安装	`msiexec /i "C:\CSS60\Client Security Solution.msi"`
不带重新引导的静默安装	`msiexec /i "C:\CSS60\Client Security Solution.msi" /qn REBOOT="R"`
静默卸载	`msiexec /x "C:\CSS60\Client Security Solution.msi" /qn`

系统迁移辅助程序安装

System Migration Assistant User's Guide 中提供对系统迁移辅助程序安装过程的描述。

Fingerprint Software 安装

可以使用以下参数启动 Fingerprint Software 程序 setup.exe 文件:

静默安装

Fingerprint Software 也可以进行静默安装。在 CD-ROM 驱动器的 Install 目录中运行 Setup.exe。

使用以下语法:

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

其中 *q* 用于静默安装，而 *i* 则用于安装。例如:

```
Setup.exe INSTALLDIR="F:\Program Files\IBM fingerprint software" /q /i
```

要卸载软件，请使用 /x 参数:

```
Setup.exe INSTALLDIR="F:\Program Files\IBM fingerprint software" /q /x
```

SMS 安装

还支持 SMS 安装。以标准方式打开 SMS 管理员控制台、创建一个新的程序包并设置程序包属性。打开程序包并在“程序”项中选择“新建程序”。在命令行中输入:

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

您可以使用用于静默安装的相同参数。

安装程序通常在安装过程结束时重新引导。如果要禁止安装期间的所有重新引导并稍后（在安装更多程序后）重新引导，将 REBOOT="ReallySuppress" 添加到属性列表中。

选项

Fingerprint Software 支持以下选项:

表 31.

参数	描述
CTRLONCE	用于只显示一次 “控制中心”。缺省值为 0。
CTLCNTR	用于在启动时运行 “控制中心”。缺省值为 1。
DEFFUS	• 0 = 不使用快速用户切换（FUS）设置 • 1 = 尝试使用 FUS 设置。 缺省值为 0。
INSTALLDIR	缺省指纹软件安装目录
OEM	• 0 = 安装服务器护照／服务器认证支持 • 1 = 仅带有本地护照的独立计算机方式
PASSPORT	安装期间设置的缺省护照类型。 • 1 = 缺省 – 本地护照 • 2 = 服务器护照 缺省值为 1。
SECURITY	• 1 = 安装安全方式支持 • 0 = 不安装; 只存在便捷方式
SHORTCUTFOLDER	“启动” 菜单中快捷方式文件夹的缺省名称
REBOOT	可用于禁止所有重新引导（包括设置为 ReallySuppress 时安装期间的提示）。

已安装软件的情况

表 32.

已安装软件	注®
客户端安全解决方案 V5.4x	这是唯一支持与 Rescue and Recovery 共存的 CSS 版本。
仅 Rescue and Recovery V3.0	• 通过完整产品安装进行安装并取消选择 CSS。 • “仅 RnR” 安装中将安装一些核心客户端安全解决方案组件以支持使用 TPM 对备份进行加密并对 PDA 主密码进行配置。
客户端安全解决方案 V6.0 单机版	• 这是一个独立的安装程序包。 • 您无法安装整个产品并通过取消选择 Rescue and Recovery 只安装客户端安全解决方案。 • CSS 组件（Private Disk 和密码管理器）是可选的。

表 32. (续)

已安装软件	注®
Rescue and Recovery V3.0 和客户端安全解决方案 V6.0	• 预装入缺省值 – 通过常规产品安装进行安装 • CSS 组件 • Private Disk 和密码管理器是可选组件

软件状态修改

表 33.

如果已安装软件是....	您要转换为.....	请按以下过程操作.....	注	构建
客户端安全解决方案 V5.4x	客户端安全解决方案 5.4x 和 Rescue and Recovery V3.0	• 安装产品。 • 仅安装 Rescue and Recovery 组件（不显示定制配置屏幕）。 • 当提示时，表明要保留已安装的客户端安全解决方案。	• 使用仿真方式实现 Rescue and Recovery 的客户端安全解决方案挂钩 • 在该方式中通过客户端安全解决方案只能获得主密码	011
客户端安全解决方案	客户端安全解决方案 6.0	• 卸载客户端安全解决方案 5.4x • 安装客户端安全解决方案 6.0 单机版	禁止尝试将客户端安全解决方案 V6.0 覆盖安装到客户端安全解决方案 V5.4x 上。将提示用户首先除去旧版本的客户端安全解决方案。	011
客户端安全解决方案	Rescue and Recovery V3.0 和客户端安全解决方案 V6.0	• 卸载客户端安全解决方案 5.4x • 安装产品。	尝试将产品覆盖安装到客户端安全解决方案 V5.4x 上会提示首先除去客户端安全解决方案 V5.4x。如果不卸载而继续安装，则只安装 Rescue and Recovery。	011

表 34.

如果已安装软件是....	您要转换为.....	请按以下过程操作.....	注	构建
Rescue and Recovery V3.0	客户端安全解决方案 5.4x 和 Rescue and Recovery V3.0	• 卸载 Rescue and Recovery • 安装客户端安全解决方案 V5.4x • 如上所述安装产品	• 客户端安全解决方案 V5.4x 不能覆盖安装到任何产品安装上。 • Rescue and Recovery V3.0 卸载过程中将删除本地备份。	011

表 34. (续)

如果已安装软件是....	您要转换为.....	请按以下过程操作.....	注	构建
Rescue and Recovery V3.0	客户端安全解决方案 6.0	• 卸载 Rescue and Recovery V3.0 • 安装客户端安全解决方案 V6.0 单机版	• 卸载 Rescue and Recovery V3.0 将删除用户文件和 CSS 注册表设置。 • 将无法再访问受 CSS 保护的 Rescue and Recovery V3.0 备份。 • Rescue and Recovery V3.0 卸载过程中将删除本地备份。 • 禁止将客户端安全解决方案 V6.0 单机版覆盖安装到任何产品安装上。 • 在这种情况下，“添加/删除程序”中的“修改”选项只允许添加客户端安全解决方案。无法通过“修改”选项除去 Rescue and Recovery。	012
Rescue and Recovery V3.0	Rescue and Recovery V3.0 和客户端安全解决方案 V6.0	• 从“添加/删除程序”选择“修改”选项。 • 添加 CSS 和任何其他组件。	• 添加 CSS 时将删除本地备份。 • 添加客户端安全解决方案时将警告用户应在添加客户端安全解决方案后制作新的备份。 • 添加客户端安全解决方案时将删除客户端安全解决方案设置和数据文件。 • 禁止将客户端安全解决方案 V6.0 单机版覆盖安装到任何产品安装上。	待定

表 35.

如果已安装软件是....	您要转换为.....	请按以下过程操作.....	注	构建
客户端安全解决方案 V6.0 单机版	客户端安全解决方案 5.4x	• 卸载客户端安全解决方案 V6.0 • 安装客户端安全解决方案 V5.4x	• 客户端安全解决方案 V5.4x 不能覆盖安装到任何产品安装上。 • 卸载客户端安全解决方案 V6.0 会提示删除数据文件和设置。此处选择的选项不影响客户端安全解决方案 V5.4x 操作。	011

表 35. (续)

如果已安装软件是....	您要转换为.....	请按以下过程操作.....	注	构建
客户端安全解决方案 V6.0 单机版	Rescue and Recovery V3.0	• 卸载客户端安全解决方案 V6.0 • 安装产品并选择“仅 Rescue and Recovery”。	• 卸载客户端安全解决方案 V6.0 会提示删除客户端安全解决方案 V6.0 用户文件和设置。 • 安装 Rescue and Recovery 3.0 会提示用户除去任何现有的客户端安全解决方案用户文件和设置。如果用户不选择除去这些文件，则取消安装。	012
客户端安全解决方案 V6.0 单机版	Rescue and Recovery V3.0 和客户端安全解决方案 V6.0	• 运行产品安装 • 无法取消选择 Rescue and Recovery 和客户端安全解决方案 选项 • 缺省情况下，已选择先前安装的客户端安全解决方案组件（密码管理器和 Private Disk），但也可以取消选择。缺省情况下，已取消选择先前未安装的组件，但也可以选择它们。	• 将在后台卸载客户端安全解决方案 V6.0 单机版。 • 将保留客户端安全解决方案 V6.0 数据文件和设置。 • 将保留仿真／非仿真状态。 • 完成产品安装后，由于先前已配置客户端安全解决方案，所以不会运行客户端安全解决方案向导。 • 使用客户端安全解决方案保护 Rescue and Recovery 备份的选项必须通过 Rescue and Recovery GUI 才能完成。最后一个安装屏幕上会提供在重新引导后运行 Rescue and Recovery GUI 的选项。 • 安装产品后，“添加/删除程序”中的选项包括“删除”、“修复”和“修改”。 • 已安装的客户端安全解决方案 V6.0 的版本必须等于或低于将安装的产品的版本，否则用户将收到消息，表示无法安装该产品。	012

注:

1. 如果用户静默安装 Rescue and Recovery 3.0，将在安装期间自动删除客户端安全解决方案用户文件和设置。
2. 在这种情况下，在产品安装期间（Rescue and Recovery 3.0 和客户端安全解决方案 6.0）选择或取消选择密码管理器和 Private Disk 决定了安装产品后组件的最终状态。

例如，如果密码管理器已与客户端安全解决方案 6.0 一起安装而用户在产品安装期间取消选择它，则完成安装后密码管理器将不再存在。如果静默运行产品安装（Rescue and Recovery 和客户端安全解决方案），除非安装命令中分别设置属性 NOPRVDISK=1 或 NOPWMANAGER=1，否则将安装密码管理器和 Private Disk。

表 36.

如果已安装软件是....	您要转换为.....	请按以下过程操作.....	注	构建
Rescue and Recovery V3.0 和客户端安全解决方案 V6.0	客户端安全解决方案 5.4x	• 卸载产品 • 安装客户端安全解决方案 V5.4x	• 客户端安全解决方案 V5.4x 不能覆盖安装到任何产品安装上。 • 卸载产品会提示删除数据文件和设置。此处选择的选项不影响客户端安全解决方案 V5.4x 操作。	011
Rescue and Recovery V3.0 和客户端安全解决方案 V6.0	Rescue and Recovery V3.0	• 从“添加/删除程序”选择“修改”选项。 • 除去客户端安全解决方案。	• 除去客户端安全解决方案时将删除本地备份。 • 卸载客户端安全解决方案将警告会丢失 PrivateDisk 和密码管理器。 • 将无法再访问受客户端安全解决方案保护的 Rescue and Recovery V3.0 备份。 • 使用“修改”除去客户端安全解决方案时将删除客户端安全解决方案设置和数据文件。	待定（不在构建 12 中）
Rescue and Recovery V3.0 和客户端安全解决方案 V6.0	客户端安全解决方案 V6.0	• 卸载产品。 • 卸载将提示删除客户端安全解决方案文件和设置。如果用户要保留现有的客户端安全解决方案配置，则可以保留这些文件和设置。 • 安装客户端安全解决方案 V6.0 单机版。	• 卸载产品。 • 卸载将提示删除客户端安全解决方案文件和设置。如果用户要保留现有的客户端安全解决方案配置，则可以保留这些文件和设置。 • 安装客户端安全解决方案 V6.0 单机版。	012

注:

1. 从“添加/删除程序”卸载客户端安全解决方案 6.0 期间或从原始源代码提供的用户界面进行卸载时，将提示用户删除 CSS 设置和数据文件。如果从命令行静默运行卸载，缺省值为删除 CSS 设置和数据文件，但是可以通过在卸载命令中设置属性 NOCSSCLEANUP=1 来覆盖该操作。

2. 从“添加/删除程序”卸载产品（Rescue and Recovery 和客户端安全解决方案 6.0）期间或从原始源代码提供的用户界面进行卸载时，将提示用户删除客户端安全解决方案设置和数据文件。如果从命令行静默运行卸载，缺省值为删除客户端安全解决方案设置和数据文件，但是可以通过在卸载命令中设置属性 NOCSSCLEANUP=1 来覆盖该操作。

第 7 章 Antidote Delivery Manager 基础结构

Antidote Delivery Manager 通过向各个系统传递来自管理员的指令并为命令提供支持来抵御病毒和蠕虫程序。管理员准备一个脚本，其中包含要在各个系统上执行的操作。存储库功能将脚本快速、安全地传递给系统并执行命令。命令包括：限制网络连接、向最终用户显示消息、从备份复原文件、下载文件、执行其他系统命令以及将机器重新引导至同一操作系统或切换入或切换出 Rescue and Recovery 环境。存储库功能和命令都可用于常规的操作系统（如 Windows XP）或 Rescue and Recovery 环境中。

抵御病毒的整体策略是缩小恶意代码的蔓延和破坏、向各个系统应用补丁和清除，然后将复原的机器重新放回网络上。对于破坏性高、传播速度快的病毒，可能需要从网络中除去受感染的系统并在 Rescue and Recovery 环境中执行所有修复操作。虽然这是最安全的方法，但如果在正常工作时间使用该方法，最终用户仍会受到影响。在某些情况下，可以通过限制网络功能来延迟或避免切换至 Rescue and Recovery 环境。下一步是为安装下载补丁和清除代码，运行无毒代码并安装补丁。一般而言，补丁是在操作系统运行时安装的，而清除和其他操作可能更适合在 Rescue and Recovery 环境中执行。完成纠正操作后，系统即可复原为正常操作，此时 Windows XP 可以运行并且网络配置得以复原。

以下两个部分详细描述了存储库操作和命令。然后阐述了该功能的安装和配置。随后的部分是一些示例，用以说明如何使用系统执行常见任务，包括：测试、对破坏性病毒做出响应、找到通过无线或虚拟专用网（VPN）连接的机器以及解决破坏性较低的问题。

存储库

存储库功能运行于各个系统上并定期检查管理员发出的新消息。它根据已调度的时间间隔或在发生几种有趣的事件（例如：引导、从暂挂或休眠状态恢复、检测到新的网络适配器以及指定新的 IP 地址）时检查消息。存储库功能在一组目录、Windows 共享位置（如 \\machine\share\directory）、HTTP URL 或 FTP URL 查找消息。如果找到多条消息，则以“按名称对目录进行排序”的顺序加以处理。每次只处理一条消息。每条消息只成功处理一次。如果消息处理失败，缺省情况下不会尝试再次处理它，但可以在消息中指定失败重试。

管理员必须将消息打包，然后将它放入由存储库功能处理的目录中。要创建程序包，管理员将构成消息的所有文件放入一个目录（或其子目录）中。必须将其中一个文件命名为主命令脚本 “GO.RRS”。管理员也可以对该消息使用签名密钥，但是如果这样，该密钥必须可用于所有目标系统。存储库功能在执行 GO.RRS 之前会检查程序包的完整性、检查签名（如果提供签名）并将所有文件解压缩到一个本地目录中。

主命令脚本文件（GO.RRS）遵循 Windows 命令文件的语法。它可能包含合法的 Windows 命令以及以下部分中列出的任何命令。还会安装一个 Python 命令解释器作为 Rescue and Recovery 环境的一部分，这样还可以从 GO.RRS 脚本调用 Python 脚本。

完成脚本执行时将删除从消息中解压缩的所有文件，因此如果在脚本退出后仍需要这些文件（例如，在重新引导后安装补丁），则必须将这些文件移动到消息目录之外。

每个系统的存储库配置都有待检查。IT 管理员可能应该将多个系统分为不同的组并为各组指定不同的存储库（网络共享）。例如，可以根据地域按近似性将系统归入文件服务器中。或者，系统可以按工程、销售或支持等功能进行分组。

Antidote Delivery Manager 命令和可用的 Windows 命令

Antidote Delivery Manager 系统提供多个用于简化系统操作的命令。除了用于创建消息和调整设置的命令之外，还包括其他命令，可分别用于控制联网、确定和控制操作系统状态、检查来自系统清单的 XML 文件以及将客户机上 Antidote Delivery Manager 脚本的进度通知最终用户。NETWK 命令可用于启用或禁用联网或将联网限制在一组限定网络地址范围内。INRR 命令可用于确定计算机正在运行 Windows XP 操作系统还是在 Rescue and Recovery 环境中。REBOOT 命令可用于关闭计算机并指定应该引导至 Windows XP 还是 Rescue and Recovery。MSGBOX 应用程序通过在弹出框中显示消息允许与最终用户进行通信。消息框可以包含“确定”和“取消”按钮，以便消息能根据最终用户的输入内容表现出不同的行为。

Antidote Delivery Manager 还提供一些 Microsoft 命令。允许的命令包括构建到命令解释程序中的所有命令（如 DIR 或 CD）。还提供其他实用命令，如用于更改注册表的 REG.EXE 以及用于验证磁盘完整性的 CHKDSK.EXE。

Antidote Delivery Manager 的典型用途

Antidote Delivery Manager 系统可用于完成各种任务。以下示例演示了如何使用该系统。

- **简单系统测试 – 显示通知**

  该系统最基本的用途是向最终用户显示单条消息。要在部署之前运行该测试并测试其他脚本，最简单的方法是将消息放在存储库中，它是管理员的个人计算机上的一个本地目录。该操作可以对脚本做出快速测试，同时不会影响到其他机器。

- **脚本准备和打包**

  在已安装 Antidote Delivery Manager 的任意机器上撰写一个 GO.RRS 脚本。请在其中包含以下一行内容：`MSGBOX /MSG "Hello World" /OK`。在包含 GO.RRS 的目录中运行 APKGMSG 命令以创建消息。

- **脚本执行**

  将消息文件放入您机器上的某个存储库目录中并遵循正确的操作。当随后运行邮件代理程序时，消息框将显示“Hello World”文本。此类脚本也是测试网络存储库以及演示功能（如从暂挂方式恢复后检查存储库）的好方法。

主要蠕虫程序攻击

该示例演示了抵御主要病毒的一种可行方法。基本方法是关闭联网、然后重新引导至 Rescue and Recovery、检索修订、执行修复、然后引导回 Windows XP 并安装补丁，最后复原联网。可以通过标志文件和 RETRYONERROR 命令使用单条消息来执行所有这些功能。

1. **锁定阶段**

   首先要完成的任务是通知最终用户即将发生的事件。如果攻击不是非常严重，管理员可以让最终用户选择将修复操作延后。在最保守的情况下，将使用该阶段来禁用

联网并提供一段较短的时间（如 15 分钟）供最终用户保存正在进行的工作。RETRYONERROR 用于将脚本保持在运行状态，随后机器可以重新引导至 Rescue and Recovery 环境中。

2. **代码分发和修复阶段**

   由于已经通过禁用网络并重新引导至 Rescue and Recovery 排除了病毒传染的威胁，因此可以检索其他代码并完成修复操作。在检索其他文件所需的时间段内可以启用网络或者只允许特定地址。在 Rescue and Recovery 中可以除去病毒文件并对注册表进行清理。不幸的是，由于补丁假定 Windows XP 正在运行，所以不能安装新的软件或补丁。此时联网仍处于禁用状态并已除去所有病毒代码，因而可以安全地重新引导至 Windows XP 以完成修复操作。此时撰写的标记文件在重新引导后将脚本带入补丁部分。

3. **补丁和恢复阶段**

   当机器重新引导至 Windows XP 中时，Antidote Delivery Manager 在最终用户可以登录之前就再次开始处理。此时应安装补丁。如果新安装的补丁需要重新引导，可以对机器进行最后一次重新引导。由于已完成所有清除和补丁安装操作，因此可以启用网络并通知最终用户能进行正常操作。

次要应用程序更新

并非所有维护都需要采取上述极端措施。如果补丁可用但是未发生病毒攻击，则可以采取较轻松的方法。

单个脚本可以通过使用 RETRYONERROR 和标记文件来控制操作。

1. **下载阶段**

   该过程首先显示一个消息框，通知最终用户将下载补丁供稍后进行安装。然后即可从服务器复制该补丁。

2. **补丁阶段**

   由于补丁代码安装已经就绪，此时应向最终用户发出警告并开始安装。如果最终用户请求延迟安装，则可以使用标记文件来跟踪延迟。稍后的安装补丁请求可能更紧急。请注意，即使最终用户关闭系统电源或重新引导系统，Antidote Delivery Manager 仍保持该状态。当最终用户授予许可权时，将根据需要安装补丁并重新引导系统。

容纳 VPN 和无线安全性

Rescue and Recovery 环境目前不支持远程访问虚拟专用网（VPN）或无线网络连接。如果某台机器在 Windows XP 中使用其中一种网络连接并重新引导至 Rescue and Recovery 中，则网络连接将丢失。因此上例中那样的脚本将不起作用，因为 Rescue and Recovery 中不提供用于下载文件和修订的联网。

解决方案是将所需的所有文件打包到原始消息中或在重新引导之前下载所需的文件。这是通过使用 GO.RRS 将所有必需的文件放入目录中完成的。该脚本文件必须确保在脚本退出之前（删除客户机上包含 GO.RRS 的目录时）将所需的文件移动到它们的最终位置。如果补丁很大，则将补丁放入消息文件中可能不可行。在这种情况下，应通知最终用户，然后将联网能力限制到包含补丁的服务器。然后，才可以在 Windows XP 中下载补丁。虽然这可能增加 Windows XP 受病毒威胁的时间，但是超出的时间也许影响并不大。

第 8 章 最佳做法

本章提供了多种使用方案以说明 Rescue and Recovery、客户端安全解决方案和 ThinkVantage Fingerprint Software 的最佳做法。该方案首先讨论硬盘驱动器的配置，其次是几个更新，然后是部署的生命周期。并对 IBM 和非 IBM 计算机上的安装情况加以描述。

安装 Rescue and Recovery 和客户端安全解决方案的部署示例

以下是在 ThinkCentre 机器和 ThinkPad 上安装 Rescue and Recovery 和客户端安全解决方案的几个示例。

ThinkCentre 部署示例

这是使用以下假设客户需求在 ThinkCentre 上进行安装的示例安装:

- **管理**
  - 使用 Rescue and Recovery 创建 Sysprep 基本备份
  - 使用本地管理员帐户来管理计算机
- **Rescue and Recovery**
  - 使用客户端安全口令来保护对 Rescue and Recovery 工作空间的访问
    - 用户必须使用其口令登录，然后可以打开他们的 SafeGuard PrivateDisk 卷文件以挽救文件
- **客户端安全解决方案**
  - 以仿真方式安装和运行
    - 并非所有 IBM 系统都配备可信平台模块（安全芯片）
  - 没有密码管理器
    - 客户使用企业单点登录解决方案来取代密码管理器
  - 启用客户端安全口令
    - 通过口令保护客户端安全解决方案应用程序
  - 启用客户端安全 Windows 登录
    - 使用客户端安全口令登录 Windows
  - 为所有用户创建 SafeGuard PrivateDisk（大小为 500 MB）
    - 每个用户需要 500 MB 空间用于安全地存储数据
  - 启用最终用户口令恢复功能
    - 使用户能通过回答用户定义的三个问题与答案来恢复口令
  - 使用 password = “XMLscriptPW” 对客户端安全解决方案 XML 脚本进行加密
    - 该密码将保护客户端安全解决方案配置文件

在准备机器上:

1. 使用 Windows “本地管理员” 帐户登录
2. 使用以下选项安装 Rescue and Recovery 和客户端安全解决方案程序:

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

注:

a. 确保一个或多个 tvt 文件（如 z062zaa1025us00.tvt）与可执行文件位于同一目录中，否则安装将失败。

b. 如果文件名为 setup_tvtrnr3_1027c.exe，表示您下载的是组合程序包。这些说明适用于可从“大企业单独语言文件”下载页面单独下载的文件。

c. 如果要执行管理安装，请参阅第 102 页的『在 Lenovo 和 IBM 品牌的计算机上新安装 Rescue and Recovery』。

3. 重新引导后，请使用 Windows 本地管理员帐户登录并准备好用于部署的 XML 脚本。从命令行运行以下命令:

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

在向导中选择以下选项:

- 选择**高级 -> 下一步**
- 选择**客户端安全口令 -> 下一步**
- 选择**使用“客户端安全登录屏幕”登录 -> 下一步**
- 输入管理员帐户的 Windows 密码 **-> 下一步**

  （例如: WPW4Admin）
- 输入管理员帐户的客户端安全口令，选中**使用客户端安全口令来保护对 Rescue and Recovery 工作空间的访问**框 **-> 下一步**

  （例如: CSPP4Admin）
- 选中**启用密码恢复**框并为管理员帐户选择三个问题和答案 **-> 下一步**

  a. 您的第一只宠物的名字是什么?

  （例如: 毛毛）

  b. 您最喜欢的电影是?

  （例如: 乱世佳人）

  c. 您最喜欢的运动队是?

  （例如: 华盛顿红人队）
- 请勿选中**使用以下选择的大小为每个用户创建一个 PrivateDisk 卷 -> 下一步**
- 查看“摘要”并选择**应用**将 xml 文件写入以下位置 C:\ThinkCentre.xml **-> 应用**
- 选择**完成**以关闭向导。

4. 在文本编辑器（XML 脚本编辑器或 Microsoft Word 2003 具有内建的 XML 格式功能）中打开以下文件并修改以下设置:

- 除去对“域”设置的所有引用。这将指示脚本使用每个系统上的本地机器名称。保存文件。

5. 通过 C:\Program Files\IBM ThinkVantage\Client Security Solution\xml_crypt_tool.exe 中找到的工具使用密码对 XML 脚本进行加密。在命令提示符处使用以下语法运行该文件:

a. xml_crypt_tool.exe C:\ThinkCentre.xml /encrypt XMLScriptPW

b. 该文件现在的名称是 C:\ThinkCentre.xml.enc 并受到 password = XMLScriptPW 的保护

现在可以将文件 C:\ThinkCentre.xml.enc 添加到部署机器中。

在部署机器上:

1. 使用 Windows 本地管理员帐户登录
2. 使用以下选项安装 Rescue and Recovery 和客户端安全解决方案程序:

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

注:

a. 确保一个或多个 tvt 文件（如 z062zaa1025us00.tvt）与可执行文件位于同一目录中，否则安装将失败。

b. 如果文件名为 setup_tvtrnr3_1027c.exe，表示您下载的是组合程序包。这些说明适用于可从 “大企业单独语言文件” 下载页面单独下载的文件。

c. 如果要执行管理安装，请参阅第 102 页的『在 Lenovo 和 IBM 品牌的计算机上新安装 Rescue and Recovery』。

3. 重新引导后，请使用 Windows 本地管理员帐户登录
4. 将先前准备好的 ThinkCentre.xml.enc 文件添加到 C:\root 目录中
5. 修改注册表，将所有用户的 SafeGuard PrivateDisk 缺省卷大小设置为 500 MB。导入 *reg* 文件即可轻松完成该操作

a. 转至: HKEY_LOCAL_MACHINE\SOFTWARE\IBM ThinkVantage\Client Security Software

b. 创建一个新的字符串值（值名称为 PrivateDiskSize，值数据为 500）

c. 创建一个 DWORD 值（值名称为 UsingPrivateDisk，值数据为 1）

6. 使用以下参数准备 RunOnceEx 命令。

- 向名为 “0001” 的 RunonceEx 键添加一个新键。它应该是: HKEY_LOCAL_MACHINE \Software\Microsoft\Windows\Current Version\RunOnceEx\0001
- 在该键中添加一个字符串值（名称为 “CSSEnroll”，值为 “c:\program files\IBM ThinkVantage\Client Security Solution\vmservere.exe” C:\ThinkCenter.xml.enc XMLscriptPW）

7. 运行 “%rr%\rrcmd.exe sysprepbackup location=L name=”Sysprep Backup””。它准备好系统之后，您将看到以下输出内容:

```
*********************************************************
** 已准备好制作 sysprep 备份。                          **
**                                                     **
** 请立即运行 SYSPREP 并关机。                          **
**                                                     **
** 下次引导机器时，它将引导至                           **
** PreDesktop Area 并制作备份。                         **
*********************************************************
```

8. 立即运行您的 Sysprep 实施。
9. 关机并重新引导机器。它将在 Windows PE 中启动备份过程。

注: 它将显示正在进行复原，但实际上正在进行备份。备份后，关闭机器电源并且不要重新启动。

Sysprep 基本备份现已完成。

Thinkpad 部署示例

这是使用以下假设客户需求在 ThinkPad 上进行安装的示例安装:

- **管理**
  - 在已经完成映像和部署的系统上安装
  - 使用域管理员帐户来管理计算机
  - 所有计算机具有 BIOS 超级用户密码 “BIOSpw”
- **客户端安全解决方案**
  - 利用可信平台模块
    - 所有机器配备安全芯片
  - 启用密码管理器
  - 禁用 SafeGuard PrivateDisk
    - 利用 Utimaco SafeGuard Easy 全面硬盘驱动器加密
  - 利用用户的 Windows 密码作为对客户端安全解决方案的认证
    - 允许使用单个 Windows 密码对 Utimaco SafeGuard Easy、客户端安全解决方案和 Windows 域进行认证
  - 使用 password = ″XMLscriptPW″ 对客户端安全解决方案 XML 脚本进行加密
    - 该密码将保护客户端安全解决方案配置文件
- **ThinkVantage Fingerprint Software**
  - 不希望利用 BIOS 和硬盘驱动器密码
  - 使用 Fingerprint 登录
    - 经过自用户登记的初始时间后，用户将切换到需要非管理员用户指纹的安全方式登录，从而有效地强制实施双因子认证方法
  - 包括指纹教程
    - 最终用户可以了解如何正确地滑动手指并获得错误操作的可视反馈

在准备机器上:

1. 从关机状态开启计算机并按 **F1** 进入 BIOS，浏览至 security（安全性）菜单并清除安全芯片。保存并退出 BIOS
2. 使用 Windows 域管理员帐户登录
3. 通过运行 f001zpz2001us00.exe 从 Web 程序包中解压缩 setup.exe 文件以安装 ThinkVantage Fingerprint Software。该操作将把 setup.exe 自动解压缩到以下位置: C:\IBMTOOLS\APPS\TFS4.6-Build1153\Application\0409\setup.exe。
4. 通过运行 f001zpz7001us00.exe 从 Web 程序包中解压缩 tutess.exe 文件以安装 ThinkVantage Fingerprint 教程。该操作将把 setup.exe 自动解压缩到以下位置: C:\IBMTOOLS\APPS\tutorial\TFS4.6-Build1153\Tutorial\0409\tutess.exe。
5. 通过运行 f001zpz5001us00.exe 从 Web 程序包中解压缩 fprconsole.exe 文件以安装 ThinkVantage Fingerprint 控制台。运行 f001zpz5001us00.exe 将把 setup.exe 自动解压缩到以下位置: C:\IBMTOOLS\APPS\fpr_con\APPS\UPEK\FPR Console\TFS4.6-Build1153\Fprconsole\fprconsole.exe。
6. 使用以下选项安装客户端安全解决方案程序:

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

7. 重新引导后，请使用 Windows 域管理员帐户登录并准备好用于部署的 XML 脚本。从命令行运行以下命令:

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

   在向导中选择以下选项以便与示例脚本保持一致:

   - 选择“高级”**-> 下一步**
   - 选择“Windows 密码” **-> 下一步**
   - 选择“使用指纹传感器登录”**-> 下一步**
   - 输入域管理员帐户的 Windows 密码 **-> 下一步**

     （例如: WPW4Admin）
   - 取消选中“启用密码恢复”**-> 下一步**
   - 查看“摘要”并选择“应用”将 xml 文件写入以下位置 C:\ThinkPad.xml
   - 选择**完成**以关闭向导
8. 通过 C:\Program Files\IBM ThinkVantage\Client Security Solution\xml_crypt_tool.exe 中找到的工具使用密码对 XML 脚本进行加密。在命令提示符处使用以下语法:

   a. xml_crypt_tool.exe C:\ThinkPad.xml /encrypt XMLScriptPW

   b. 该文件现在的名称是 C:\ThinkPad.xml.enc 并受到 password = XMLScriptPW 的保护

在部署机器上:

1. 使用公司的软件分发工具来部署 ThinkVantage Fingerprint Software 可执行文件 setup.exe，该文件从准备机器解压缩到每台部署机器上。将 setup.exe 推送到机器时，使用以下命令进行安装:

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

2. 使用公司的软件分发工具来部署 ThinkVantage Fingerprint 教程可执行文件 tutess.exe，该文件从准备机器解压缩到每台部署机器上。将 tutess.exe 推送到机器时，使用以下命令进行安装:

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

3. 使用公司的软件分发工具来部署 ThinkVantage Fingerprint 控制台可执行文件 fprconsole.exe，该文件从准备机器解压缩到每台部署机器上。

   - 将 fprconsole.exe 文件放入 “C:\Program Files\ThinkVantage Fingerprint Software\” 目录中
   - 通过运行以下命令关闭 BIOS 开机安全支持: fprconsole.exe settings TBX 0
4. 使用公司的软件分发工具来部署 ThinkVantage 客户端安全解决方案可执行文件 “setup_tvtcss6_1027.exe”。

   - 将 setup_tvtcss6_1027.exe 推送到机器时，通过以下命令进行安装: setup_tvtcss6_1027.exe /s /v”/qn NOPRVDISK=1 NOCSSWIZARD=1 SUPERVISORPW=”BIOSpw”””
   - 软件安装将自动启用可信平台模块硬件。
5. 重新引导系统后，使用以下过程通过 XML 脚本文件对系统进行配置:

   - 将先前准备好的 ThinkPad.xml.enc 文件复制到 C:\ 目录中。

- 运行 C:\Program Files\IBM ThinkVantage\Client Security Solution\vmserver.exe C:\ThinkPad.xml.enc XMLScriptPW

6. 重新引导后，系统即可进行客户端安全解决方案用户登记。每个用户可以使用其用户标识和 Windows 密码登录系统。将自动提示登录系统的每个用户登记到客户端安全解决方案中，然后才能登记到指纹识别器中。
7. 当系统的所有用户都登记到 ThinkVantage Fingerprint Software 中后，即可启用“安全方式”设置以强制所有 Windows 非管理员用户使用其指纹登录。
   - 运行以下命令: C:\Program Files\ThinkVantage Fingerprint Software\fprconsole.exe settings securemode 1
   - 要除去消息“按 CTRL+ALT+DEL 使用密码登录”，请在登录屏幕中运行以下命令:

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

客户端安全解决方案 6.0 和 ThinkVantage Fingerprint Software 的部署现已完成。

在 Lenovo 和 IBM 品牌的计算机上新安装 Rescue and Recovery

这一部分描述了新安装 Rescue and Recovery。

准备硬盘驱动器

部署系统时首先要考虑的是准备提供者系统的硬盘驱动器。为确保一切是从清洁的硬盘开始的，您必须清除主硬盘上的主引导记录。

1. 从提供者系统中除去所有存储设备（如辅助硬盘、USB 硬盘、USB 存储钥匙以及 PC 卡存储器等），要安装 Windows 的主硬盘除外。

   警告: 运行该命令将擦除目标硬盘驱动器上的全部内容。运行之后，您将无法从目标硬盘驱动器恢复任何数据。
2. 创建 DOS 引导软盘并将 CLEANDRV.EXE 文件放置在其中。
3. 引导软盘（唯一一个连接的存储设备）。在 DOS 提示符处输入以下命令:

   ```
   CLEANDRV /HDD=0
   ```
4. 安装操作系统和应用程序。就像不准备安装 Rescue and Recovery 那样构建提供者系统。该过程中的最后一步是安装 Rescue and Recovery。

安装

安装过程中的第一步是将 InstallShield 可执行文件解压缩到 C:\RRTEMP 目录。如果您要在多个系统上安装 Rescue and Recovery，则执行该过程一次大致可以将每台机器上的安装时间缩短一半。

1. 假定安装文件位于 C 盘的根目录中，请创建文件 EXE_EXTRACT.CMD，它将把文件 C:\SETUP_TVTRNR3_*XXXX*.EXE（其中 *XXXX* 为构建标识）解压缩到 C:\RRTEMP 目录中:

   ```
   :: 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. 您可以在安装 Rescue and Recovery 之前执行许多定制操作。该方案中的一些示例是:
   - 将增量备份的最大数量更改为 4。
   - 将 Rescue and Recovery 设置为每天下午 1:59 执行到本地硬盘的增量备份并将它命名为 “Scheduled”。
   - 对不在本地 “管理员组” 中的所有用户隐藏 Rescue and Recovery 用户界面。
3. 创建定制 TVT.TXT 文件。您可以修改某些参数。有关更多信息，请参阅第 121 页的附录 B, 『TVT.TXT 设置和值』。

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

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


[RescueRecovery]
LastBackupLocation=1
CustomPartitions=0
Exclude=0
Include=0
MaxNumberOfIncrementalBackups=5
EncryptUsingCSS=0
HideCSSEncrypt=0
UUIDMatchRequired=0
PasswordRequired=0
DisableSchedule=0
DisableRestore=0
DisableSFR=0
DisableViewBackups=0
DisableArchive=0
DisableExclude=0
DisableSingleStorage=0
DisableMigrate=0
DisableDelete=0
DisableAnalyze=0
DisableSysprep=1
CPUPriority=3
Yield=0
Ver=4.1
DisableBackupLocation=0
DeletedBackupLocation=0
HideLocationNotFoundMsg=0
HideMissedBackupMessage=0
```

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

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

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

4. 在定制 TVT.TXT 文件所在的同一目录中，创建 INSTALL.CMD 文件，它将执行几项操作:
   - 将定制 TVT.TXT 文件复制到 C:\RRTemp 目录中已创建的安装程序包中:
   - 执行 Rescue and Recovery 的静默安装（结束时不重新引导）。
   - 启动 Rescue and Recovery，以便执行基本备份。
   - 启动服务后，设置环境以创建 Rescue and Recovery CD 的 ISO 映像（这通常作为重新引导的一部分执行）。
   - 创建 ISO 映像。
   - 创建基本备份并重新引导系统。
5. 修改 INSTALL.CMD 代码。以下内容表示 INSTALL.CMD 的代码:

```
:: 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
```

注: 如果系统重新引导，则不需要设置环境。

```
:: 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
```

定制

您在环境中部署了 Rescue and Recovery 并且希望使用 Rescue and Recovery 更改以下各项:

- 您需要 4 个以上的增量备份并要将它更改为 10 个。
- 下午 1:59 的备份时间对您的环境造成一定程度的干扰。您要将时间更改为上午 10:24。
- 您希望系统上的所有用户都能访问 Rescue and Recovery 3.0 用户界面。
- 您希望在已调度的备份过程中使系统服从于其他进程。您在试验之后做出的评估确定在您的环境中 Yield= 的正确值应该是 2 而不是标准值 0。

要在多台机器上做出这些更改:

1. 使用以下内容创建一个名为 UPDATE.MOD 的 mod 文件（请使用文本编辑器）:

```
[RescueRecovery] MaxNumberOfIncrementalBackups=10

[rescuerecovery] ScheduleHour=10

[rescuerecovery] ScheduleMinute=24

[rescuerecovery] GUIGroup=

[rescuerecovery] Yield=2
```

2. 您可以随后创建一个 INSTALL.CMD 文件并使用您选择的系统管理工具将 INSTALL.CMD 和 UPDATE.MOD 文件推送到目标系统。当系统运行 INSTALL.CMD 文件之后，更新将生效。INSTALL.CMD 文件的内容如下:

```
:: 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"
```

更新

您可能需要对系统做出较大的更改，例如，对 Windows 进行 service pack 更新。在安装 service pack 之前，通过执行以下步骤在系统上强制进行增量备份并按名称找到该备份:

1. 创建 FORCE_BU.CMD 文件并将它向下推送到目标系统。
2. 当 FORCE_BU.CMD 文件出现在目标系统上时，立即启动它。

FORCE_BU.CMD 文件的内容为:

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

启用 Rescue and Recovery 桌面

在意识到 Rescue and Recovery 的优点一段时间后，您可能希望从 Rescue and Recovery 环境受益。为了进行演示，我们在以下部分中提供一个样本 UPDATE_RRE.CMD 脚本（它将解压缩 Rescue and Recovery 环境的控制文件），您可以编辑该文件并随后使用 RRUTIL.exe 将它放回 Rescue and Recovery 环境中。有关更多信息，请参阅第 18 页的『使用 RRUTIL.EXE』。

要修改 Pre Desktop Area，UPDATE_RRE.CMD 脚本演示了几个过程:

- 使用 RRUTIL.exe 从 Rescue and Recovery 环境获取文件。要从 Rescue and Recovery 环境解压缩的文件由文件 GETLIST.TXT 定义。
- 在编辑完相应的文件后，创建一个目录结构以便将文件放回 Pre Desktop Area 中。
- 安全起见，请为文件制作一个副本，然后对文件进行编辑。

在该示例中，您要更改当最终用户单击 Rescue and Recovery 环境中的**打开浏览器**按钮时打开的主页。Web 页面 `http://www.lenovo.com/thinkvantage` 打开。

要做出更改，当使用“记事本”打开 PEACCESSIBMEN.INI 文件时:

1. 将以下行:

```
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__
```

更改为

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

2. 将文件的新版本放入目录结构中，以便将文件放入 Rescue and Recovery 环境中。有关详细信息，请参阅第 18 页的『使用 RRUTIL.EXE』。
3. 将系统重新引导至 Rescue and Recovery 环境中。
4. 您已完成一些分析并确定某些文件必须备份，而其他文件则不需要备份，因为它们驻留在服务器上并且可以在系统复原后获得。要这样做，请创建定制 IBMFILTER.TXT 文件。该文件与 NSF.CMD 文件放在同一目录中，后者将它复制到正确的位置，如以下示例所示:

   NSF.CMD:

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

   IBMFILTER.TXT:

   ```
   x=*.nsf
   ```

表 37. UPDATE_RR.CMD 脚本

```
@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

文件将自动打开

pause
:: Make a copy of original file
copy
c:\RRDeployGuide\GuideExample\RROriginal\preboot\usrintfc\PEAccessIBMen.ini
c:\RRDeployGuide\GuideExample\RROriginal\preboot\usrintfc\
PEAccessIBMen.original.ini
notepad
c:\RRDeployGuide\GuideExample\RROriginal\preboot\usrintfc\PEAccessIBMen.ini
pause
copy c:\RRDeployGuide\GuideExample\RROriginal\preboot\usrintfc\
PEAccessIBMen.ini c:\RRDeployGuide\GuideExample\put\preboot\usrintfc
:: 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

创建 GETLIST.TXT:

\preboot\usrintfc\PEAccessIBMen.ini
```

在非 IBM 品牌的计算机上安装 Rescue and Recovery

要安装 Rescue and Recovery，硬盘上的主引导记录中必须有八个可用扇区。Rescue and Recovery 使用定制“引导管理器”以进入“恢复”区域中。

某些 OEM 将指针存储到主引导记录扇区中的产品恢复代码中。OEM 产品恢复代码可能会影响 Rescue and Recovery 引导管理器的安装。

请考虑以下方案和最佳做法以帮助您确保 Rescue and Recovery 提供所需的功能和特性:

硬盘驱动器设置的最佳做法: 方案 1

该方案描述各种新的映像部署，其中包括 Rescue and Recovery。如果将 Rescue and Recovery 部署到包含 OEM 产品恢复代码的现有 OEM 客户机，请运行以下测试以确定 OEM 产品恢复代码是否会影响 Rescue and Recovery:

1. 用包含 OEM 产品恢复代码的映像安装测试客户机。
2. 安装 Rescue and Recovery。如果 OEM 产品恢复代码使得 MBR 中没有八个可用扇区，您将看到以下错误消息:

   ```
   错误 1722。该 Windows Installer 程序
   包存在问题。作为安装程序的一部分运行的某个
   程序未能正常完成。请联系相关人
   员或程序包供应商。
   ```

如果使用的是基本操作系统的 OEM 映像，请确保“主引导记录”不包含产品恢复数据。您可以通过以下方式进行操作:

注意: 运行以下命令将擦除目标硬盘驱动器的全部内容。运行之后，您将无法从目标硬盘驱动器恢复任何数据。

1. 使用可从

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

   的 administrative tools（管理工具）部分提供的 CLEANDRV.EXE 文件来确保计划用于创建基本映像的硬盘驱动器上的主引导记录已清除所有扇区。
2. 根据您的部署过程打包映像。

硬盘驱动器设置的最佳做法: 方案 2

在现有客户机上部署 Rescue and Recovery 程序则需要投入一些精力并做出规划。

如果您收到错误 1722 并需要创建八个可用扇区，请致电 IBM 技术支持以报告错误并获得进一步指示。

创建可引导 Rescue and Recovery CD

Rescue and Recovery 根据当前服务区域内容（而不是预装的 ISO 映像）构建并刻录挽救介质 CD。然而，如果相应的 ISO 映像已存在，因为它已预先载入或者因为先前它已构建过，该映像将用于刻录 CD，而不是新建一个映像进行刻录。

由于涉及资源问题，在任何给定的时间只能运行一个 CD 刻录应用程序的实例。如果某个实例正在运行，则尝试启动第二个实例将产生错误消息，并且第二个实例将异常终止。另外，由于访问硬盘驱动器的受保护区域的性质，只有管理员才能创建 ISO; 但是受限用户可以将 ISO 刻录到 CD。恢复 CD 上将包括以下文件和目录:

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

- scrrec.ver

注: 如果创建新的 ISO 映像，则系统驱动器上至少必须有 400 MB 的可用空间才能复制目录树并构建 ISO。对如此之多的数据进行处理将导致很密集的硬盘操作，并且在某些计算机上可能需要 15 分钟或更多的时间。

创建恢复 ISO 文件并将样本脚本文件刻录成 CD: 准备以下代码:

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

注: 仅当系统在安装后没有重新引导时才需要以下七行代码（以粗体显示）。

```
:: 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
```

将 Rescue and Recovery 安装到 12 型服务分区中

您必须具有以下条件才能将 Rescue and Recovery 安装到 12 型服务分区中:

- SP.PQI 文件。该文件包含用于创建服务分区的基本可引导文件。
- PowerQuest PQDeploy
- Rescue and Recovery 的最新安装程序

在服务分区中安装 Rescue and Recovery 环境提供几个相关的选项。

注: 12 型分区必须驻留在上一次使用的条目中，该条目位于包含 Windows 的同一驱动器的分区表中。可以使用 bmgr32 /info 来确定 12 型分区在 HDD 上的驻留位置。有关更多信息，请参阅第 140 页的『Rescue and Recovery 引导管理器控制（BMGR32）』。

要执行安装，请完成以下过程:

1. 在驱动器末尾至少保留 700 MB 未分配的可用空间。
2. 使用 PowerQuest 将 SP™.PQI 文件复原到未分配的可用空间。
3. 删除步骤 1 中创建的主分区（C 盘除外），然后重新引导。

   注: 系统卷信息可能在新创建的服务分区上。需要通过 “Windows 系统复原” 删除系统卷信息。

4. 安装 Rescue and Recovery 并根据提示重新引导。

Sysprep 备份 / 复原

请注意，密码持久性无法与 Sysprep 备份 / 复原一起使用。

完成 Sysprep 备份后，应关闭并重新引导系统。

Computrace 和 Rescue and Recovery

在非 BIOS 系统上，安装 Computrace 后将无法卸载 Rescue and Recovery。

第 9 章 Fingerprint Software

Fingerprint 控制台必须从 Fingerprint Software 安装文件夹中运行。基本语法是 FPRCONSOLE [USER | SETTINGS]。USER 或 SETTINGS 命令指定了将使用的操作集。 “fprconsole user add TestUser /FORCED” 就是一个完整的命令。如果命令未知或是未指定所有参数，则显示简短命令列表和参数。

要下载 Fingerprint Software 和管理控制台，请使用以下链接:

http://www.lenovo.com/think/support/site.wss/document.do?sitestyle=lenovo&indocid=TVAN-EAPFPR

特定于用户的命令

要登记或编辑用户，请使用 USER 部分。如果当前用户没有管理员权限，则控制台行为取决于 FS 的安全方式。便捷方式: 标准用户可以使用 ADD、EDIT 和 DELETE 命令。但用户只可以修改自己的护照（以其用户名登记的护照）。安全方式: 不允许任何命令。语法:

```
FPRCONSOLE USER command
```

其中 *command* 是以下某个命令: ADD、EDIT、DELETE、LIST、IMPORT 和 EXPORT。

表 38.

命令	语法	描述	示例
登记新用户	ADD [*username* [| *domain**username*]] [/FORCED]	/FORCED 标志将禁用向导的 “取消” 按钮，以确保成功完成登记。如果不指定用户名，则使用当前用户名。	fprconsole add domain0\testuser fprconsole add testuser fprconsole add testuser /FORCED
编辑已登记用户	EDIT [*username* [| *domain**username*]]	如果不指定用户名，则使用当前用户名。 **注**: 所编辑的用户首先必须验证其指纹。	fprconsole edit domain0\testuser fprconsole edit testuser
删除用户	DELETE [*username* [| *domain**username* | /ALL]]	/ALL 标志将删除该计算机上登记的所有用户。如果不指定用户名，则使用当前用户名。	fprconsole delete domain0\testuser fprconsole delete testuser fprconsole delete /ALL
枚举已登记用户	List		
将已登记用户导出到文件	EXPORT username [| domain\username] file	该命令将已登记用户导出到 HDD 上的某个文件。随后可以在其他计算机或同一计算机（如果删除了用户）上使用 IMPORT 命令将用户导入。	

表 38. (续)

命令	语法	描述	示例
导入已登记用户	IMPORT *file*	导入命令将从指定的文件导入用户。 **注**: 如果文件中的用户已使用相同的指纹在同一计算机上登记，则无法确保哪个用户在识别操作中的优先级更高。	

全局设置命令

可以使用 SETTINGS 部分更改 Fingerprint Software 的全局设置。该部分中的所有命令都需要管理员权限。语法为:

FPRCONSOLE SETTINGS *command*

其中 *command* 是以下某个命令: SECUREMODE、LOGON、CAD、TBX 和 SSO。

表 39.

命令	描述	语法	示例
安全方式	该设置用于在 Fingerprint Software 的便捷方式和安全方式之间进行切换。	SECUREMODE 0|1	要设置为便捷方式: fprconsole settings securemode 0
登录类型	该设置启用（1）或禁用（0）登录应用程序。如果使用 /FUS 参数，则启用“快速用户切换”方式中的登录（如果计算机配置允许）。	LOGON 0|1 [/FUS]	
CTRL+ALT+DEL 消息	该设置启用（1）或禁用（0）登录中的“按 CTRL+ALT+DEL”文本。	CAD 0|1	
开机安全	该设置全局关闭（0）Fingerprint Software 中的开机安全支持。当关闭开机安全支持时，不会显示任何开机安全向导或页面并且 BIOS 设置情况如何也无关紧要。	TBX 0|1	
开机安全单点登录	该设置启用（1）或禁用（0）登录中 BIOS 中使用的指纹，当用户通过 BIOS 中的验证时便会自动登录。	SSO 0|1	

安全方式与便捷方式

ThinkVantage Fingerprint Software 能以两种安全方式运行: 便捷方式和安全方式。

便捷方式适用于家用计算机，这类计算机不需要很高的安全级别。所有用户都可以执行任何操作，其中包括编辑其他用户的护照以及使用密码登录系统的可能性（不必进行指纹认证）。

安全方式适用于要实现更高安全性的情况。一些特殊功能是专为管理员保留的。只有管理员可以使用密码登录而不必进行其他认证。

*管理员*是本地管理员组的任意成员。设置安全方式后，只有管理员可以将它切换回简单方式。

安全方式 – 管理员

如果在登录时输入了错误的用户名或密码，安全方式会显示消息“只有管理员才能以用户名和密码登录该计算机”。这是为了增强安全性并且避免向黑客提供信息，告知他们无法登录的原因。

表 40.

指纹	**描述**
创建新护照	管理员可以创建自己的护照，也可以创建受限用户的护照。
编辑护照	管理员只可以编辑自己的护照。
删除护照	管理员可以删除所有受限用户和其他管理员的护照。如果其他用户使用的是开机安全，则管理员此时可以选择从开机安全中除去用户模板。
开机安全	管理员可以删除开机时使用的受限用户和管理员指纹。 **注:** 启用开机方式时，至少必须有一个指纹。
设置	
登录设置	管理员可以对所有登录设置做出更改。
受保护的屏幕保护程序	管理员可以访问。
护照类型	管理员可以访问 – 只与服务器相关。
安全方式	管理员可以在安全方式和便捷方式之间进行切换。
Pro Server	管理员可以访问 – 只与服务器相关。

安全方式 – 受限用户

在 Windows 登录过程中，受限用户必须使用指纹登录。如果受限用户的指纹识别器无法正常使用，管理员需要将 Fingerprint Software 设置更改为便捷方式以启用用户名和密码访问。

表 41.

指纹	
创建新护照	受限用户无法访问。
编辑护照	受限用户只可以编辑自己的护照。
删除护照	受限用户只可以删除自己的护照。
开机安全	受限用户无法访问。

表 41. (续)

指纹	
设置	
登录设置	受限用户不可以修改登录设置。
受保护的屏幕保护程序	受限用户可以访问。
护照类型	受限用户无法访问。
安全方式	受限用户不可以修改安全方式。
Pro Server	受限用户可以访问 – 只与服务器相关。

便捷方式 – 管理员

在 Windows 登录过程中，管理员可以使用他们的用户名和密码或指纹登录。

表 42.

指纹	
创建新护照	管理员只可以创建自己的护照。
编辑护照	管理员只可以编辑自己的护照。
删除护照	管理员只可以删除自己的护照。
开机安全	管理员可以删除开机时使用的受限用户和管理员指纹。 **注:** 启用开机方式时，至少必须有一个指纹。
设置	
登录设置	管理员可以对所有登录设置做出更改。
受保护的屏幕保护程序	管理员可以访问。
护照类型	管理员可以访问 – 只与服务器相关。
安全方式	管理员可以在安全方式和便捷方式之间进行切换。
Pro Server	管理员可以访问 – 只与服务器相关。

便捷方式 – 受限用户

在 Windows 登录过程中，受限用户可以使用他们的用户名和密码或指纹登录。

表 43.

指纹	
创建新护照	受限用户只可以创建自己的护照。
编辑护照	受限用户只可以编辑自己的护照。
删除护照	受限用户只可以删除自己的护照。
开机安全	受限用户只可以删除自己的指纹。
设置	
登录设置	受限用户不可以修改登录设置。
受保护的屏幕保护程序	受限用户可以访问。
护照类型	受限用户不可以访问 – 只与服务器相关。
安全方式	受限用户不可以修改安全方式。

表 43. (续)

指纹	
Pro Server	受限用户可以访问 – 只与服务器相关。

ThinkVantage Fingerprint Software 和 Novell Netware Client

ThinkVantage Fingerprint Software 与 Novell 用户名及密码必须匹配。

如果您在计算机上安装了 ThinkVantage Fingerprint Software，然后再安装 Novell Netware Client，则可能会覆盖注册表中的某些项。如果您在登录 ThinkVantage Fingerprint Software 时遇到问题，请转至“登录设置”屏幕并重新启用“登录保护程序”。

如果您在计算机上安装了 Novell Netware Client，但在安装 ThinkVantage Fingerprint Software 之前还未登录客户机，将显示“Novell 登录”屏幕。提供屏幕请求的信息。

要更改“登录保护程序设置”：

- 启动“控制中心”。
- 单击**设置**。
- 单击**登录设置**。
- 启用或禁用“登录保护程序”。

  如果要使用指纹登录，请选中“以受指纹保护的登录取代 Windows 登录”复选框。请注意，启用和禁用“登录保护程序”需要重新引导。
- 启用或禁用快速用户切换（如果系统支持）。
- （可选功能）对开机引导安全认证的用户启用或禁用自动登录。
- 设置 Novell 登录设置。登录 Novell 网络时提供以下设置:
  - **已激活**

    ThinkVantage Fingerprint Software 自动提供已知安全证书。如果 Novell 登录失败，将显示 Novell Client 登录屏幕并提示输入正确的数据。
  - **登录过程中询问**

    ThinkVantage Fingerprint Software 显示 Novell Client 登录屏幕并提示输入登录数据。
  - **已禁用**

    ThinkVantage Fingerprint Software 不尝试 Novell 登录。

附录 A. 安装命令行参数

Microsoft Windows Installer 通过命令行参数提供多项管理员功能。

管理安装过程和命令行参数

Windows Installer 可以针对网络执行应用程序或产品的管理安装以供工作组使用或用于定制。对于 Rescue and Recovery 安装程序包，管理安装将安装源文件解压缩到指定的位置。

- 要运行管理安装，请使用 /a 参数从命令行执行安装程序包:

  ```
  Setup.exe /a
  ```

管理安装会显示一个向导，提示管理用户指定安装文件的解压缩位置。缺省解压缩位置是 C:\。可以选择新的位置，该位置可能包含 C:\ 以外的驱动器（其他本地驱动器，映射的网络驱动器等）。也可以在该步骤中创建新目录。

- 要静默运行管理安装，则可以在命令行上设置公共属性 TARGETDIR 以指定解压缩位置:

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

  或

  ```
  msiexec.exe /i "IBM Rescue and Recovery.msi" /qn TARGERDIR=F:\IBMRR
  ```

完成管理安装后，管理员可以定制源文件（例如，向 TVT.TXT 添加设置）。

使用 MSIEXEC.EXE

要在定制后使用解压缩的源文件进行安装，用户从命令行调用 MSIEXEC.EXE，传递解压缩的 *.MSI 文件的名称。MSIEXEC.EXE 是用于解释安装程序包并在目标系统上安装产品的安装程序的可执行程序。

```
msiexec /i "C:\WindowsFolder\Profiles\UserName\
Personal\MySetups\project name\product configuration\release name\
DiskImages\Disk1\product name.msi"
```

注: 在一行中输入以上命令并且斜杠后没有空格。

第 118 页的表 44 描述了可以与 MSIEXEC.EXE 结合使用的可用命令行参数及其使用方法的示例。

表 44. 命令行参数

参数	描述

/I *package*
或
product code
	使用该格式安装产品:
	`Othello:msiexec /i "C:\`*`WindowsFolder`*`\Profiles\`
	`UserName``\Personal\MySetups`
	`\Othello\Trial Version\`
	`Release\DiskImages\Disk1\`
	`Othello Beta.msi"`
	
	Product Code 指在产品项目视图的 Product Code 属性中自动生成的 GUID。

/a *package*	**/a** 选项允许具备管理员权限的用户将产品安装到网络。
/x *package* 或 *product code*	**/x** 选项卸载产品。
/L [i|w|e|a|r|u|c|m|p|v|+] *log file*	使用 **/L** 选项进行构建会指定到日志文件的路径; 这些标志表明要记录到日志文件中的信息: • **i** 记录状态消息 • **w** 记录非致命警告消息 • **e** 记录任何错误消息 • **a** 记录操作序列的起始 • **r** 记录特定于操作的记录 • **u** 记录用户请求 • **c** 记录初始用户界面参数 • **m** 记录内存不足信息 • **p** 记录终端设置 • **v** 记录详细输出设置 • **+** 追加到现有文件 • ***** 是通配符, 它允许您记录所有信息（详细输出设置除外）
/q [n|b|r|f]	/q 选项用于结合以下标志设置用户界面级别: • **q** 或 qn 不创建用户界面 • **qb** 创建基本用户界面 以下的用户界面设置在安装结束时显示模态对话框: • **qr** 显示精简的用户界面 • **qf** 显示完整的用户界面 • **qn+** 不显示用户界面 • **qb+** 显示基本用户界面
/? 或 /h	两个命令都显示 Windows Installer 版权信息

表 44. 命令行参数 (续)

参数	描述

TRANSFORMS	使用 **TRANSFORMS** 命令行参数指定要应用于基础包的任何转换。转换命令行调用可能类似于以下情况:
	`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"`
	可以使用分号分隔多个转换。因此，建议您不要在转换名称中使用分号，因为 Windows Installer 服务无法对它们做出正确的解释。

属性	所有公共属性都可以从命令行进行设置或修改。公共属性是全部大写的，以示与专用属性的区别。例如，*COMPANYNAME* 为公共属性。
	要从命令行设置属性，请使用以下语法:
	`PROPERTY=VALUE`
	如果要更改 *COMPANYNAME* 的值，则输入以下语句:
	`msiexec /i "C:\WindowsFolder\`
	`Profiles\UserName\Personal`
	`\`
	`MySetups\Your Project Name\`
	`Trial Version\My Release-1`
	`\`
	`DiskImages\Disk1\ProductName.msi"`
	`COMPANYNAME="InstallShield"`

附录 B. TVT.TXT 设置和值

以下缺省值为建议的设置。值对于不同配置可能不同（例如: 预装入、Web 下载和 OEM 版本）。以下安装配置设置可用:

表 45. TVT.TXT 设置和值

设置	值
AccessFile （请参阅 GUIGroup）	*filename*，其中 *filename* 是包含 Windows 本地组（不是域组）名称的文件的标准路径，这些组有权执行 Rescue and Recovery 操作。如果留空或不使用，能登录计算机的所有用户都可以启动 GUI 并执行命令行操作。缺省情况下，该文件留空。
BackupPartition	0 = 指定驱动器上的第一分区 1 = 指定驱动器上的第二分区 2 = 指定驱动器上的第三分区 3 = 指定驱动器上的第四分区 以下部分中指定了驱动器: [BackupDisk] = 本地硬盘驱动器 [SecondDisk] = 辅助本地硬盘驱动器 [USBDisk] = USB 硬盘驱动器 **注**: 分区必须已经存在。如果未设置，则将提示用户建立分区（如果在用户界面选定目标驱动器时该目标驱动器上存在多个分区）。
BatteryPercentRequired	范围从 0 到 100。缺省值为 100。
CPUPriority	*n*，其中 *n* = 1 到 5; 1 是最低优先级，而 5 是最高优先级。 缺省值为 3。
CustomPartitions	0 = 备份每个分区 1 = 查看每个分区中的 IncludeInBackup
DisableAnalyze	0 = 显示 “优化备份存储器 optionEnable 归档” 1 = 隐藏该选项 缺省值为 0。
DisableArchive	0 = 启用归档 1 = 隐藏归档 缺省值为 0。

表 45. TVT.TXT 设置和值 (续)

设置	值
DisableBackupLocation	0 = 启用所有目标 0x01 = 禁用本地目标 0x02 = 禁用 CD/DVD 驱动器 0x08 = 禁用 USB/HDD 0x10 = 禁用网络 0x20 = 禁用辅助 HDD 1 = 隐藏归档 可以结合这些值使多个位置变灰。例如，值 0x0A 将禁用 CD/DVD 和 USB HDD; 值 0x38 将禁用 USB HDD、网络和辅助 HDD。如果只要启用到本地硬盘驱动器的备份，可以使用 0x3A（甚至 0xFE）。
DisableBootDisc	0 = 在创建 CD/DVD 备份时创建可引导 CD 1 = 不创建可引导 CD “禁用引导光盘”功能仅适用于备份，不适用于归档。
DisableDelete	0 = 显示“删除备份”选项 1 = 隐藏该选项 缺省值为 0。
DisableExclude	0 = 显示“排除文件／文件夹”选项 1 = 隐藏“排除文件／文件夹”选项 缺省值为 0。
DisableLiveUpdate	0 = 显示“即时更新”选项 1 = 隐藏该选项 缺省值为 0。
DisableMigrate	0 = 显示“从备份创建迁移文件” 1 = 隐藏该选项 缺省值为 0。
DisableRestore	0 = 启用复原 1 = 隐藏复原 缺省值为 0。
DisableSchedule	0 = 显示“备份调度”选项 1 = 隐藏“备份调度”选项 缺省值为 0。

表 45. TVT.TXT 设置和值 (续)

设置	值
DisableSFR	0 = 启用单一文件复原 1 = 隐藏单一文件复原 缺省值为 0。
DisableSingleStorage	0 = 显示“单一存储”选项 1 = 隐藏该选项 缺省值为 0。
DisableViewBackups	0 = 显示“查看备份”选项 1 = 隐藏该选项 缺省值为 0。
DisableVerifyDisc	0 = 验证光学写操作 1 = 不验证光学写操作 缺省值为 0。
Exclude （请参阅 Include）	0 = 不应用 GUIEXCLD.TXT 1 = 应用 GUIEXCLD.TXT **注:** 1. 排除和选择文件可以在安装之前定义并在安装过程中应用。 2. Exclude 和 Include 不能同时为 1。
GUIGroup （请参阅 AccessFile）	*group*，其中 *group* 是 Windows 本地组（不是域组），该组有权执行 Rescue and Recovery 操作。授权组列表存储在 AccessFile 条目定义的文件中。
HideAdminBackups	0 = 在列表中显示管理员备份。 1 = 隐藏管理员备份。 缺省值为 0。
HideBaseFromDelete	0 = 在“删除备份”对话框中显示基本备份。 1 = 在“删除备份”对话框中隐藏基本备份。 缺省值为 0。
HideBootUSBDialog	0 = 如果备份到 USB HDD 并且它不可引导，则显示提示 1 = 隐藏提示 缺省值为 0。
HideDiffFileSystems	0 = 复原 / 保存文件时显示 FAT/FAT32 分区 1 = 复原 / 保存文件时隐藏 FAT/FAT32 分区 缺省值为 0。

表 45. TVT.TXT 设置和值 (续)

设置	值
HideCSSEncrypt	0 = 使用客户端安全解决方案时不隐藏加密备份 1 = 使用客户端安全解决方案时隐藏加密备份 缺省值为 0。
HideGUI	0 = 对授权用户显示 GUI 1 = 对所有用户隐藏 GUI
HideLocationNotFoundMessage	0 = 显示对话框消息 1 = 隐藏对话框消息 缺省值为 0。
HideLockHardDisk	0 = 显示“保护硬盘免受 MBR 损坏”选项 1 = 隐藏该选项 缺省值为 1。
HideMissedBackupMessages	0 = 显示对话框 1 = 隐藏对话框 缺省值为 1。
HideNoBatteryMessage	0 = 显示消息 1 = 隐藏消息 缺省值为 1。
HideNumBackupsDialog	0 = 不隐藏当用户到达最大备份数时显示的对话框 1 = 隐藏当用户到达最大备份数时显示的对话框 缺省值为 1。
HidePowerLossBackupMessage	0 = 显示备份掉电消息 1 = 隐藏消息 缺省值为 0。
HidePasswordPersistence	0 = 隐藏 GUI 1 = 显示 GUI 缺省值为 0。
HidePasswordProtect	0 = 显示“密码保护”复选框。 1 = 隐藏“密码保护”复选框。 缺省值为 0。
HideSuspendCheck	0 = 不隐藏“将计算机从暂挂／休眠唤醒”复选框 1 = 隐藏该复选框 缺省值为 1。

表 45. TVT.TXT 设置和值 (续)

设置	值
Include （请参阅 Exclude）	0 = 不应用 GUIINCLD.TXT 1 = 应用 GUIINCLD.TXT 并显示设置包含文件和文件夹的选项 **注:** 1. 排除和选择文件可以在安装之前定义并在安装过程中应用。 2. Exclude 和 Include 不能同时为 1。
LocalBackup2Location	*x\foldername*，其中 *x* 是盘符，而 *foldername* 是任何标准文件夹名称。 缺省值为: *1st partition letter on the second drive*:\IBMBackupData **注:** 1. 由于盘符可能随着时间发生变化，Rescue and Recovery 在安装时将盘符与分区相关联，然后使用分区信息而不是盘符。 2. 这是 TaskParameters 条目的位置字段。
LockHardDisk	0 = 不锁定硬盘以保护 MBR 1 = 锁定硬盘 缺省值为 0。
MaxBackupSizeEnforced	*x*，其中 *x* 是以 GB 计的大小。该值将不阻止备份超出该阈值。然而，如果超出了阈值，则下次执行“随需应变的”备份时将警告用户文件大小。缺省值为 0。
MaxNumberOf IncrementalBackups	缺省 = 5，最小 = 2，最大 = 32
MinAnalyzeFileSize *n*	其中 *n* 是“优化备份存储器空间”屏幕上向用户显示的文件的最小文件大小（以 MB 为单位）。缺省值为 20。
NetworkUNCPath	网络共享使用以下格式: *\\computername\sharefolder* 没有缺省值。 **注:** 该位置将不受“文件过滤驱动程序”的保护。
NetworkUNCPath	*server share name*，例如: \\MYSERVER\SHARE\FOLDER
NumMinutes	*x*，表示 *x* 分钟后运行任务。
PasswordRequired	0 = 打开 Rescue and Recovery 环境不需要密码。 1 = 打开 Rescue and Recovery 环境需要密码。
PDAPreRestore	*cmd*，其中 *cmd* 是复原操作之前要在 Rescue and Recovery 环境中运行的程序的标准路径。
PDAPreRestore *n*	*cmd*，其中 *cmd* 是复原操作之前要在 Rescue and Recovery 环境中运行的程序的标准路径。
PDAPreRestoreParameters	要在 PDARestore 程序中使用的参数。
PDAPreRestoreParameters *n*	要在 PDARestore 程序中使用的参数。
PDAPreRestoreShow	0 = 隐藏任务 1 = 显示任务

表 45. TVT.TXT 设置和值 (续)

设置	值
PDAPreRestoreShow *n*	0 = 隐藏任务 1 = 显示任务
PDAPostRestore	*cmd*，其中 *cmd* 是复原操作之前要在 Rescue and Recovery 环境中运行的程序的标准路径。
PDAPostRestore *n*	*cmd*，其中 *cmd* 是复原操作之前要在 Rescue and Recovery 环境中运行的程序的标准路径。
PDAPostRestoreParameters	要在 PDARestore 程序中使用的参数。
PDAPostRestoreParameters *n*	要在 PDARestore 程序中使用的参数。
PDAPostRestoreShow	0 = 隐藏任务 1 = 显示任务
PDAPostRestoreShow *n*	0 = 隐藏任务 1 = 显示任务
Post （请参阅 PostParameters）	*cmd*，其中 *cmd* 是要在主任务之后运行的可执行文件的标准路径。
Post （请参阅 PostParameters）*n*	其中 *n* 是备份编号 0、1、2、3...32 *cmd*，其中 *cmd* 是要在主任务之后运行的可执行文件的标准路径。 例如: • Post0=command.bat *path* 它在基本备份之后运行 • Post1=command.bat *path* 它在增量备份之后运行 **注**: 仅适用于备份
PostParameters （请参阅 Post）	*cmd*，其中 *cmd* 是要在主任务之后运行的可执行文件的标准路径。仅适用于备份。
PostParameters *n*（请参阅 Post）	*parms*，其中 *parms* 是要在后任务中使用的参数
	parms，其中 *parms* 是要在后任务中使用的参数。 **注**: 仅适用于备份
PostRestore	*cmd*，其中 *cmd* 是完成复原操作之后要在 Windows 中运行的程序的标准路径。
PostRestore *n*	*cmd*，其中 *cmd* 是完成复原操作之后要在 Windows 中运行的程序的标准路径。
PostRestoreParameters	要在 PostRestore 程序中使用的参数
PostRestoreParameters *n*	要在 PostRestore 程序中使用的参数
PostRestoreShow	0 = 隐藏复原任务 1 = 显示复原任务
PostRestoreShow *n*	0 = 隐藏复原任务 1 = 显示复原任务

表 45. TVT.TXT 设置和值 (续)

设置	值
PostShow	0 = 隐藏后任务 1 = 显示后任务 缺省值为 0。
PostShow *n*	0 = 隐藏后任务 1 = 显示后任务 缺省值为 0。 其中 *n* 是备份编号 0、1、2、3....32 **注**: 仅适用于备份
Pre （请参阅 PreParameters）	*cmd*，其中 *cmd* 是要在主任务之前运行的可执行文件的标准路径。
Pre （请参阅 PreParameters）*n*	其中 *n* 是备份编号 0、1、2、3....32 *cmd*，其中 *cmd* 是要在主任务之前运行的可执行文件的标准路径。 例如: • Pre0=command.bat *path* 它在基本备份之前运行 • Pre1=command.bat *path* 它在增量备份之前运行 **注**: 仅适用于备份。
PreParameters （请参阅 Pre）	其中 *parms* 是要在预任务中使用的参数
PreRejuvenate *cmd*	其中 *cmd* 是系统重生操作之前要在 Windows 中运行的程序的标准路径。
PreRejuvenateParameters *parms*	其中 *parms* 是要在 PreRejuvenate 程序中使用的参数。
PreRejuvenateShow	0 = 隐藏任务 1 = 显示任务
PostRejuvenate *cmd*	*cmd*，其中 *cmd* 是系统重生操作之后要在 Windows 中运行的程序的标准路径。
PostRejuvenateParameters *parms*	其中 *parms* 是要在 PostRejuvenate 程序中使用的参数。
PostRejuvenateShow	0 = 隐藏任务 1 = 显示任务
PreShow	0 = 隐藏预任务 1 = 显示预任务 缺省值为 1。

表 45. TVT.TXT 设置和值 (续)

设置	值
PreShow *n*	其中 *n* 是备份编号 0、1、2、3....32 *cmd*，其中 *cmd* 是要在主任务之前运行的可执行文件的标准路径。 **注:** 仅适用于备份
PreWinRestore	*cmd*，其中 *cmd* 是复原操作之前要在 Windows 中运行的程序的标准路径。
PreWinRestore *n*	*cmd*，其中 *cmd* 是复原操作之前要在 Windows 中运行的程序的标准路径。
PreWinRestoreParameters	要在 PreWinRestore 程序中使用的参数
PreWinRestoreParameters *n*	要在 PreWinRestore 程序中使用的参数
PreWinRestoreShow	0 = 隐藏后任务 1 = 显示后任务
PreWinRestoreShow *n*	0 = 隐藏后任务 1 = 显示后任务
ResumePowerLossBackup	0 = 如果上一次备份过程中掉电，则不继续备份进程 1 = 继续备份 缺省值为 1。
RunBaseBackup	0 = 不执行基本备份 1 = 执行基本备份 缺省值为 0。 `runbasebackuplocation=(Location)` 值为: L = 本地 U = USB N = 网络 S = 辅助 HDD C = CD
ScheduleDayOfTheMonth	*x*，其中 *x* 等于 1 到 28 或 35（仅适用于每月备份）。35 = 每月最后一天

表 45. TVT.TXT 设置和值 (续)

设置	值
ScheduleDayOfTheWeek	仅对于每周备份 0 = 星期日 1 = 星期一 2 = 星期二 3 = 星期三 4 = 星期四 5 = 星期五 6 = 星期六 缺省值为 0（星期日）。
ScheduleFrequency	0 = 未调度 1 = 每天 2 = 每周 3 = 每月 缺省值为 2（每周）。
ScheduleHour	*x*，其中 *x* 等于 0 到 23（0 是 0:00，12 是中午，23 是晚上 11:00）。 缺省值为 0。
ScheduleMinute	*x*，其中 *x* 等于 0 到 59（递增），表示一小时中启动增量备份的分值。 缺省值为 0。
ScheduleWakeForBackup	0 = 不唤醒计算机执行已调度备份 1 = 如果是用于已调度备份的台式机，则唤醒它，但不唤醒笔记本计算机 2 = 唤醒计算机而不管是台式机还是笔记本计算机 缺省值为 2。 **注**：如果笔记本计算机因为备份被唤醒，但交流电源未删除，则在备份操作开始前它将返回到暂挂／休眠状态。

表 45. TVT.TXT 设置和值 (续)

设置	值
ScheduleMode	*x*，其中 *x* 是具有以下某个值的位掩码: • 0 = 无调度 • 0x01 = 每分钟 • 0x04 = 每周 • 0x08 = 每月 • 0x10 = 每当启动服务时（通常为每次引导机器时） • 0x20 = 机器从暂挂／休眠中醒来 • 0x40 = USB HDD 变为已连接 • 0x80 = 网络变为已连接 • 0x100 = 网络变为已断开连接 • 0x200 = BIOS 密码重新设置 • 0x400 = 主板更换 当用户更改 GUI 中的值时，将自动更新该参数。如果通过手动更改 TVT.TXT 文件或脚本编制更改了 ScheduleFrequency 值，reloadsched 将更新该参数。 **注:** 不需要设置 USB HDD 变为已连接或网络变为已连接位即可将备份从本地硬盘驱动器自动同步到 USB HDD 或网络。
SkipLockedFiles	0 = 遇到锁定文件和受损文件时显示对话框 1 = 始终跳过锁定文件和受损文件
SPBackupLocation=2	用于设置服务分区的备份。 如果不使用该设置，则取出引导 CD、复原 CD 以及除去服务分区上的其他数据时将复原缺省的 500MB 服务分区。
Task	*cmd*，其中 *cmd* 是要作为主任务运行的程序的标准路径。 **注:** 任务数量不能超出 50。
TaskParameter	*parms* 是要在任务中使用的参数。
TaskShow	0 = 隐藏任务 1 = 显示任务 缺省值为 0。
UUIDMatchRequired	0 = 不需要计算机 UUID 匹配。 1 = 需要计算机 UUID 匹配。 **注:** 当 UUIDMatchRequired 设置为 1 时捕获的备份将继续需要 UUID 匹配（即使该设置稍后做了更改）。
Yield	*n*，其中 *n* 等于 0 到 8; 0 表示 Rescue and Recovery 不产出，8 表示 Rescue and Recovery 生成最大产出值。 **注:** 较高产出将逐渐减缓备份性能并提供更好的交互性能。 缺省值为 0。

在安装 Rescue and Recovery 后，以下配置可以在位于已安装的目录中的 TVT.TXT 文件中进行更改。将使用在安装过程中指定的值初始化这些配置。

TVT.txt 备份和复原

为了支持静默安装，使用安装前编辑好的外部文件（*TVT.TXT*）来定义 Rescue and Recovery 备份和复原配置。TVT.TXT 文件将遵循标准的 Windows .ini 文件格式，其数据按节（用 [] 表示）组织并且每行一个条目（格式为 “setting=value” ）。Rescue and Recovery 将使用产品名称作为节标题（如 Rapid Restore Ultra）。另外，可以在安装之前定义包含 / 排除过滤文件并在安装过程中应用它。

如果 IT 管理员要使用设置来定制他们的备份，他们应编辑安装目录中的 TVT.TXT 文件。执行该操作的最佳时机是在安装 Rescue and Recovery 之前或在它安装之后以及第一次备份之前。每个备份位置都包含一个 TVT.TXT 文件。第一次备份之前，只有一个 TVT.TXT 文件。如果使用该方法，所有备份将包含全部更改并且不会遇到任何 TVT.TXT 版本和同步问题。有时必须在备份之后编辑 TVT.TXT 文件。在这种情况下，有两种方法可以使用最新更改来更新所有 TVT.TXT 文件。IT 管理员可以将安装目录 TVT.TXT 文件复制到所有备份文件夹中或启动另一个备份，该过程将自动实现所有 TVT.TXT 版本与安装目录版本的同步。第二种方法更好。

调度备份和相关的任务

调度程序并不是专为 Rescue and Recovery 设计的。然而，配置存储在同一 TVT.TXT 文件中。当安装 Rescue and Recovery 后，它将对调度程序批量载入相应的设置。

以下是对调度程序结构的描述:

- 位置: 安装文件夹
- 每个已调度作业的条目
- 要运行的脚本
- 用于进度通知的已命名管道（可选）
- 调度信息（每月、每周、每天、工作日、周末 – 多个调度; 例如，可以通过创建两个调度来支持星期二和星期五）
- 要传递给功能的变量

请考虑以下示例: 对于按调度执行增量备份的 Rescue and Recovery，以下条目使用备份之前和之后的回调为应用程序提供相应的指示:

```
[SCHEDULER]

Task1=rescuerecovery

[rescuerecovery]

Task="c:\program
files\ibm\Rescue and Recovery\

rrcmd.exebackup.bat"

TaskParameters=BACKUP location=L name="Scheduled"

ScheduleFrequency=2

ScheduleDayOfTheMonth=31

ScheduleDayOfTheWeek=2

ScheduleHour=20

ScheduleMinute=0

ScheduleWakeForBackup=0

Pre="c:\program files\antivirus\scan.exe"
```

```
Post="c:\program files\logger\log.bat"
```

管理不同的 TVT.txt 文件

由于硬盘驱动器可以包含多个分区，因此备份和复原程序需要知道使用哪个分区来存储备份数据。如果特定目标包含多个分区并且将把备份操作制成脚本，则需要在备份操作之前配置以下设置。如果用户可以启动备份操作，则可以忽略这一部分。

对于到本地硬盘驱动器的备份，可以在 TVT.TXT 文件的 BackupDisk 节中找到配置设置。到本地辅助硬盘驱动器的备份使用 SecondDisk 节，而到 USB HDD 的备份使用 USBDisk 节，如下所示:

```
BackupPartition=x
```

其中 *x* 是范围 0 - 3，其中 0 表示相应驱动器上的第一个分区。

注: 分区必须已经存在。如果不设置，当选择 GUI 中相应的目标时，将提示用户是否存在多个分区。例如，如果要备份到 USB HDD 上的辅助分区，则 TVT.TXT 文件条目应该如下所示:

```
[USBDisk]
BackupPartition=1
```

映射网络驱动器用于备份

映射网络驱动器功能依赖于 C:\Program Files\IBM ThinkVantage\Common\MND 目录中的 MAPDRV.INI 文件。所有信息存储在 DriveInfo 节。

“通用命名约定”（UNC）条目包含试图连接的位置的计算机名称和共享。

NetPath 条目是来自 mapdrv.exe 的输出。它包含进行连接时使用的实际名称。

User 和 Pwd 条目是用户名和密码条目。它们是加密的。

以下是映射网络驱动器的示例条目:

```
[DriveInfo]
UNC=\\server\share
NetPath=\\9.88.77.66\share
User=116226064151192077230149185054220105210064012092037082020 15...
Pwd=1162260641510000000001491850542201052100640120920370820201 5...
```

为了部署，该文件可以复制到将使用相同用户名和密码的多台计算机上。Rapid Restore Ultra 根据 TVT.TXT 中的值覆盖 UNC 条目。

设置网络备份的用户帐户

当在网络共享上创建 RRBACKUPS 目录时，服务使该目录成为只读文件夹并为它指定访问权，从而确保只有创建该文件夹的帐户对它具有完全控制权。

要完成合并操作，用户帐户必须具有“移动”许可权。如果不是以最初创建该文件夹的帐户（如管理员）登录，则合并过程将失败。

附录 C. 命令行工具

ThinkVantage 技术功能也可以由公司 IT 管理员通过命令行界面进行本地或远程调用。可以通过远程文本文件设置来维护配置设置。

Antidote Delivery Manager

Mailman

该程序使用命令 C:\program files|IBM ThinkVantage\Rescue and Recovery\ADM\mailman.exe。它将检查 Antidote 存储库中是否存在要运行的任务。没有命令行参数。

Antidote 向导

命令 AWizard.exe 位于管理员安装它的任何位置。没有命令行参数。

设置密码

有关密码的讨论，请参阅第 30 页的『密码』。

CFGMOD

CFGMOD 提供使用脚本更新 TVT.TXT 文件的方法。CFGMOD 命令位于 C:\Program Files\IBM ThinkVantage\Rescue and Recovery\ 目录中。如果您修改备份调度，则该命令后必须跟有 RELOADSCHED。该实用程序必须用管理员权限运行。

语法:

```
cfgmod TVT.TXT mod file
```

mod 文件的格式需要每条目占一行。每个条目包括节号（用 [和] 定界），然后依次为参数名称、 “=” 和值。例如，要调整备份调度，mod 文件条目可以改为:

```
[rescuerecovery]ScheduleFrequency=1
[rescuerecovery]ScheduleHour=8
[rescuerecovery]ScheduleMinute=0
```

客户端安全解决方案

客户端安全解决方案具有以下命令行工具:

SafeGuard PrivateDisk

该命令行界面位于 C:\Program Files\IBM ThinkVantage\SafeGuard PrivateDisk\ 文件夹中。语法为:

```
PDCMD
 [ADDCERT volumename /pw adminpassword /sn certSN [/acc access]]  |
 [LIST]  |
 [MOUNT volumename [/pw userpassword [/pt authmode]] [/ro]]  |
```

```
[NEW volumename [/sz size] [/dl driveletter] [/fs filesystem]
  [/pw adminpassword] [/pwu userpassword]]  |
[UNMOUNT volumename /f]  |
[UNMOUNTALL [/f]]  |
[SETPASSWORD volumename /pw adminpassword /pwu userpassword [/ro]]
```

表 46 中显示了参数:

表 46.

参数	结果
ADDCDERT	向 PrivateDisk 卷添加证书
LIST	为该用户列出 PrivateDisk 卷
MOUNT	安装特定 PrivateDisk 卷
NEW	创建新的 PrivateDisk 卷
UNMOUNT	卸装特定 PrivateDisk 卷
UNMOUNTALL	卸装所有 PrivateDisk 卷
SETPASSWORD	设置 PrivateDisk 卷上的用户密码
volumename	包含 PrivateDisk 文件的卷的名称
pw	密码
sn	证书的序列号
acc	要添加的证书的访问类型。有效值为: • **adm** 管理员访问 • **uro** 用户只读访问 • **usr** 用户写访问（缺省值）
pt	认证方法。有效值为: • **0** 管理员访问（缺省值） • **1** 用户密码 • **2** 基于证书的登录的 PIN
ro	只读
sz	大小（以千字节为单位）
dl	PrivateDisk 卷的盘符（缺省值 = 下一个可用盘符）
fs	文件系统。缺省值为: • FAT（缺省值） • NTFS
pwu	用户密码

表 46. (续)

参数	结果
f	强制操作

Security Advisor

要从 GUI 运行它，请单击**开始 -> 程序 -> ThinkVantage -> 客户端安全解决方案**。单击**高级**，然后选择**审计安全性设置**。它将运行 C:\Program Files\IBM ThinkVantage\Common\WST\wst.exe 进行缺省安装。

参数为:

表 47.

参数	描述
HardwarePasswords	可以是 1 或 0，1 将显示该节，0 将隐藏该节。如果未输入值，则根据缺省情况进行显示。
PowerOnPassword	设置值，表明应启用开机密码，否则将对设置做出标志。
HardDrivePassword	设置值，表明应启用硬盘驱动器密码，否则将对设置做出标志。
AdministratorPassword	设置值，表明应启用管理员密码，否则将对设置做出标志。
WindowsUsersPasswords	可以是 1 或 0，1 将显示该节，0 将隐藏该节。如果未输入值，则根据缺省情况进行显示。
Password	设置值，表明应启用用户密码，否则将对设置做出标志。
PasswordAge	设置值，表明该机器上应使用的 Windows 密码寿命，否则将对设置做出标志。
PasswordNeverExpires	设置值，表明 Windows 密码始终不会到期，否则将对设置做出标志。
WindowsPasswordPolicy	可以是 1 或 0，1 将显示该节，0 将隐藏该节。如果未输入值，则根据缺省情况进行显示。
MinimumPasswordLength	设置值，表明该机器上应使用的密码长度，否则将对设置做出标志。
MaximumPasswordAge	设置值，表明该机器上应使用的密码寿命，否则将对设置做出标志。
ScreenSaver	可以是 1 或 0，1 将显示该节，0 将隐藏该节。如果未输入值，则根据缺省情况进行显示。
ScreenSaverPasswordSet	设置值，表明屏幕保护程序应使用密码，否则将对设置做出标志。
ScreenSaverTimeout	设置值，表明该机器上的屏幕保护程序应使用的超时，否则将对设置做出标志。

表 47. (续)

参数	描述
FileSharing	可以是 1 或 0，1 将显示该节，0 将隐藏该节。如果未输入值，则根据缺省情况进行显示。
AuthorizedAccessOnly	设置值，表明应该为文件共享设置授权访问，否则将对设置做出标志。
ClientSecurity	可以是 1 或 0，1 将显示该节，0 将隐藏该节。如果未输入值，则根据缺省情况进行显示。
EmbeddedSecurityChip	设置值，表明应启用安全芯片，否则将对设置做出标志。
ClientSecuritySolution	设置值，表明该机器上应使用的 CSS 版本，否则将对设置做出标志。

所有值的另一个选项是 ignore（忽略）,它表示显示值，但在比较中不包含该值。当 Security Advisor 运行时，一个 HTML 文件将写入 c:\ibmshare\wst.html，一个原始数据 XML 文件将写入 c:\ibmshare\wst.xml。

示例

以下是一个 [WST] 节，它显示了所有节并将所有设置设为它们的缺省值:

```
[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
```

要隐藏或定制 Security Advisor，请在 TVT.txt 文件中添加一个名为 WST 的节。您可以隐藏或定制多个值，但必须将它们添加到 TVT.txt 文件中。

如果不希望使用 Security Advisor 并且不希望它在 GUI 中显示为“已启用”，请删除以下可执行文件:

```
C:\Program Files\IBM ThinkVantage\Common\WST\wst.exe
```

证书转移向导

如果不希望使用证书转移向导并且不希望它在 GUI 中显示为“已启用”，请删除以下可执行文件:

```
C:\Program Files\IBM ThinkVantage\Client Security Solution
\certificatetransferwizard.exe
```

客户端安全向导

该向导用于获取硬件所有权、配置软件和登记用户。它还用于通过 XML 文件生成部署脚本。可以通过运行以下命令来了解该向导的功能:

```
C:\Program Files\IBM ThinkVantage\Client Security Solution\css_wizard.exe /?
```

表 48.

参数	结果
/h 或 /?	显示帮助消息框
/name:*FILENAME*	放置在生成的部署文件的标准路径和文件名之前。文件扩展名为 .xml。
/encrypt	使用 AES 加密对脚本文件进行加密。如果对文件加密，将为文件名追加扩展名 .enc。如果不使用 /pass 命令，则使用静态口令来掩盖此文件。
/pass:	放置在用于保护已加密部署文件的口令之前。
/novalidate	禁用向导的密码和口令检查功能，这样即可在已配置的机器上创建脚本文件。例如，当前机器上的管理员密码可能不是希望用于企业范围的管理员密码。使用 /novalidate 命令使您能够在创建 xml 文件时在 css_wizard GUI 中输入一个不同的管理员密码。

以下是该命令的示例:

```
css_wizarde.exe /encrypt /pass:my secret /name:C:\DeployScript /novalidate
```

注: 如果系统以仿真方式运行，则可执行文件名为 css_wizard.exe。

部署文件加密 / 解密工具

该工具用于对客户端安全 XML 部署文件进行加密 / 解密。可以通过运行以下命令来了解该工具的功能:

```
C:\Program Files\IBM ThinkVantage\Client Security Solution\xml_crypt_tool.exe. /?
```

表 49 中显示了参数:

表 49.

参数	结果
/h 或 /?	显示帮助消息
FILENAME	标准路径名以及扩展名为 .xml 或 .enc 的文件名
encrypt 或 decrypt	为 .xml 文件选择 /encrypt，为 .enc 文件选择 /decrypt

表 49. (续)

参数	结果
PASSPHRASE	可选参数（如果使用口令来保护文件，它是必需的）。

示例:

```
xml_crypt_tool.exe "C:\DeployScript.xml" /encrypt "my secret"
```

以及

```
xml_crypt_tool.exe "C:\DeployScript.xml.enc" /decrypt "my secret"
```

部署文件处理工具

工具 vmserver.exe 用于处理客户端安全 XML 部署脚本。可以通过运行以下命令来了解该工具的功能:

```
C:\Program Files\IBM ThinkVantage\Client Security Solution\vmserver.exe /?
```

表 50.

参数	结果
FILENAME	FILENAME 参数必须具有文件扩展名 xml 或 enc
PASSPHRASE	PASSPHRASE 参数用于对扩展名为 enc 的文件进行解密

以下是该命令的示例:

```
Vmservere.exe  C:\DeployScript.xml.enc "my secret"
```

注: 如果系统以仿真方式运行，则可执行文件名为 vmserver.exe。

TPMENABLE.EXE

TPMENABLE.EXE 文件用于打开或关闭安全芯片。

表 51.

参数	描述
/enable 或 /disable（打开或关闭安全芯片）	打开或关闭安全芯片。
/quiet	隐藏 BIOS 密码或错误提示
sp:*password*	BIOS 管理员 / 超级用户密码（不要用引号括起密码）

样本命令:

```
tpmenable.exe /enable /quiet /sp:My BiosPW
```

eGatherer

eGatherer 命令位于 C:\Program Files\IBM ThinkVantage\common\egatherer\egather2.exe。

egather2.exe 使用收集到的信息创建 EG2 输出。它还可以创建本地 XML 输出文件（存储在主文件夹中）。请注意，EG2 文件使用内部格式。

将创建两个 XML 文件，一个用于系统信息，另一个用于人口统计信息。通过将制造商、型号和序列号组合在一起创建出 XML 文件的名称。例如：IBM-2373Q1U-99MA4L7.XML，IBM-2373Q1U-99MA4L7.DEMOGRAPHICS.XML。

可以使用以下命令行语法从命令行执行扫描程序:

egather2.exe [-help] [-batch] [-silent] [-nolimit] [-local] [-listprobes] [-probe probename *probename*]

- **-help**

  显示简短的帮助消息。
- **-batch**

  不显示免责声明。
- **-silent**

  在操作过程中不显示任何内容。
- **-nolimit**

  收集整个事件日志。缺省值为最新的 500 个条目。
- **-local**

  创建本地 XML 文件。
- **-listprobes**

  列出可用的探测。
- **-probe**

  运行指定的探测。

MAPDRV

MAPDRV 命令将调用用户界面以映射网络驱动器。MAPDRV.EXE 命令位于 C:\Program Files\IBM ThinkVantage\Common\MND 目录中。映射网络驱动器界面支持以下参数:

语法:

```
mapdrv [开关]
```

不带参数输入该命令将启动该应用程序，用户必须手动输入信息。

所有参数的返回码为:

- **0** = 成功
- **> 0** = 失败

表 52. MAPDRV 参数

参数	结果
/nodrive	进行网络连接而不为连接指定盘符
/pwd	该用户在此共享上的密码。
/set	设置备份和复原使用的共享、用户和密码。

表 52. MAPDRV 参数 (续)

参数	结果
/s	静默。不管是否进行连接都不提示用户。
/timeout	设置超时值。
/unc	共享名称，格式为 \\server\share
/user	该共享的用户名。

使用 /SET 命令时，将把以下节添加到 TVT.TXT 文件中。使用 /UNC/USER 和 PWD 参数的以下示例说明了这一点:

```
mapdrv /set /unc sharename /user username /pwd password
[mapdrv]
UNC=\\test\test
User=1EE22597AE4D
PWD=04E22197B34D95943ED5A169A0407C5C
```

Rescue and Recovery 引导管理器控制（BMGR32）

引导管理器界面命令行界面是 BMGR32。它驻留在目录 C:\Program Files\IBM ThinkVantage\Common\BMGR 中。下表列出了 BMGR32 的开关及其结果。

表 53. BMGR32 参数

bmgr32	结果
/B0	引导至分区 0（基于分区表中的顺序）
/B1	引导至分区 1
/B2	引导至分区 2
/B3	引导至分区 3
/BS	引导至服务分区
/BW	引导至 Rescue and Recovery 受保护分区
/BWIN	重置引导至 WINPE 的请求。必须在引导之前调用它。
/CFG*file*	应用配置文件参数。有关配置文件的详细信息，请参阅第 143 页的『RRCMD 命令行界面』。
/DS	返回 MBR 数据扇区（从 0 开始）
/D*n*	将更改应用到磁盘 n，其中 n 从 0 开始（缺省值: 如果未定义 “SystemDrive”，则为包含环境变量 “SystemDrive” 或 “C:\” 的磁盘）
/H0	隐藏分区 0
/H1	隐藏分区 1
/H2	隐藏分区 2
/H3	隐藏分区 3
/HS	隐藏服务分区
/P12	通过将分区类型设置为 12 来隐藏服务分区
/INFO	显示 HDD 信息（检查 8 个可用扇区）
/INFOP	显示 HDD 信息（检查 16 个可用扇区）
/M0	Rescue and Recovery 环境位于服务分区中

表 53. BMGR32 参数 (续)

bmgr32	结果
/M1	Rescue and Recovery 环境位于 C:\PARTITION（双引导 Windows 和 Windows PE）
/M2	Rescue and Recovery 环境位于带有 DOS 的服务分区中（双引导 Windows PE 和 DOS; 仅限 Lenovo 或 IBM 品牌的预装入）
/OEM	计算机不是 IBM 或 Lenovo 品牌的计算机。这会在开机自检后对 F11（缺省）按键强制再次检查。这可能是较旧的 IBM 品牌的系统必需的。这也是 OEM 版本的 Rescue and Recovery 的缺省设置。
/Patch*n*	仅用于安装程序以设置 MBR 补丁程序可以访问的变量。
Patchfile*filename*	仅用于安装程序以安装 MBR 补丁
/PRTC	仅用于安装程序以检索补丁返回码
/IBM	系统是 IBM 或 Lenovo 品牌的计算机
/Q	静默
/V	详细
/R	重新引导计算机
/REFRESH	重置数据扇区中的分区表条目
/TOC *tocvalue*	设置 BIOS TOC 位置（表示 8 个字节数据的 16 个字符）
/U0	显示分区 0
/U1	显示分区 1
/U2	显示分区 2
/U3	显示分区 3
/US	显示服务分区
/F*mbr*	装入 RRE 主引导记录程序
/U	卸装 RRE 主引导记录程序
/UF	强制安装或卸载 MBR 程序
/?	列出命令行选项。

使用 /info 属性调用 bmgr.exe 时，将转储以下信息:

- **其他 MBR**

  包含 MBR 的扇区编号（第一个扇区除外）。
- **数据**

  MBR 使用的数据扇区的扇区编号。
- **补丁索引**

  使用 MBR 应用的任何补丁的扇区编号。
- **校验和返回**

  如果没有校验和错误，它应该为 0。
- **引导分区**

  服务分区从 1 开始的分区表索引。

- **备用分区**

  指向 DOS 可引导区域的分区表索引（如果存在）。
- **原始 MBR**

  存储机器的原始 MBR 的扇区编号。
- **IBM 标志**

  来自数据扇区的值（如果是 IBM 或 Lenovo 品牌的系统，则为 1；否则为 0）
- **引导配置**

  描述用于说明机器布局的安装选项。无论使用服务分区，还是虚拟分区。
- **特征符**

  数据扇区和第一个扇区中找到的特征符值（应包含 “NP” ）。
- **暂停持续时间**

  这是屏幕显示 F11 消息时等待的 ¼ 秒的数量。
- **扫描码**

  引导至服务区域时使用的键。85 用于 F11 键。
- **RR**

  BMGR 不使用它，它是由 Rescue and Recovery 设置的。
- **先前活动分区**

  引导至服务区域时，该值包含先前活动分区的分区表索引。
- **引导状态**

  MBR 使用它来确定机器的当前状态。0 – 引导至常规操作系统，1 – 引导至服务操作系统，2 – 从服务操作系统引导回常规操作系统。
- **备用引导标志**

  引导至备用操作系统（如 DOS）。
- **先前分区类型**

  引导至服务区域时，此值包含引导至服务区域之前服务分区设置成的分区类型。
- **优先 IBM MBR 索引**

  由安装程序使用。
- **补丁 IN: OUT**

  来自补丁代码的输入和输出值（如果使用）。
- **F11 消息**

  向用户显示的消息（如果不支持正确的 BIOS 调用）。

RELOADSCHED

该命令重新装入 TVT.TXT 中定义的已调度设置。如果您对 TVT.TXT 做出调度更改，则必须执行该命令以激活更改。

样本命令:

```
C:\Program Files\IBM ThinkVantage\Rescue and Recovery\reloadsched
```

RRCMD 命令行界面

主 Rescue and Recovery 命令行界面是 RRCMD。该命令位于 C:\Program Files\IBM ThinkVantage\Rescue and Recovery\reloadsched.exe 子目录中。请参阅以下信息以使用 Rescue and Recovery 的命令行界面。

语法:

RRcmd *command filter=filterfile location=c* [name=*abc* | level=*x*] [silent]

表 54. RRcmd 参数

命令	结果
Backup	启动常规备份操作（必须包含 location 和 name 参数）
Restore	启动常规复原操作（必须包含 location 和 level）
List	列出备份级别中包含的文件（必须包含 location 和 level）
Basebackup	启动备用基本备份。它不会用作增量备份的基础（必须包含 location、name 和 level）。level 必须小于 99。如果已存在另一个 level 相同的基本备份，将覆盖它。
Sysprepbackup	当重新引导计算机后，在 Pre Desktop Area 中登台备份操作。该功能主要用于捕获 Sysprep 备份。 **注:** 1. 进度条有时不会移动。如果发生这种情况，您可以通过侦听硬盘驱动器来验证是否正在进行备份。当备份完成时，您会收到消息表明备份已完成。 2. 如果您在将 sysprep 备份创建到网络时设置了密码，则只有在制作增量备份后，才会把密码文件写到备份位置。以下是两个变通办法: a. 创建一个本地 sysprep 备份并将备份复制到网络或 USB。 b. 在 sysprep 备份后，将增量备份创建到网络或 USB 并保留或删除增量备份。
Copy	将备份从一个位置复制到另一个位置。这又称为“归档”（必须包含 location）。
Rejuvenate	将操作系统系统重生到指定的备份
Delete	删除备份（必须包含 location）
Changebase	根据 file.txt 的内容更改所有备份中的文件。file.txt 中的选项为: **A** 添加 **D** 删除 **RS** 替换

表 54. RRcmd 参数 (续)

命令	结果
`migrate`	从备份创建迁移文件
`filter=filterfile`	识别将复原的文件和文件夹，同时不改变其他文件。它只与 **restore** 命令一起使用。
`Location=c`	可选择以下一个或多个带有相关结果的选项。 **L** 用于主本地硬盘驱动器 **U** 用于 USB HDD **S** 用语辅助本地硬盘驱动器 **N** 用于网络 **C** 用于 CD/DVD 复原
`name=abc`	其中 *abc* 是备份的名称
`level=x`	其中 *x* 是从 0（基本）到增量备份最大数（只与复原选项一起使用）之间的数字。对于备份命令，仅当执行管理员备份时才需要 level=*x* 命令（例如，等于或大于 100）。 **注**: 1. 要从最新的备份进行复原，请勿提供该参数。 2. 所有备份和复原功能通过该服务传递以保持正确的秩序（如执行回调）。命令行选项将取代备份命令。

引导管理器配置文件格式	引导管理器配置文件的格式与先前版本的引导管理器保持向后兼容。以下未显示的任何开关都不受支持。文件格式是一个每个条目各占一行的文本文件。
	`<PROMPT1=this is the text that will appear on F11 prompt>`
	`<KEY1=F11>`
	`<WAIT=40>`

系统迁移辅助程序

该模块是与旧的 SMA4.2 SMABAT.EXE 保持兼容的命令行程序。该模块的命令参数和控制卡（Commands.TXT）应与 SMA 4.2 保持兼容。

Active Update

Active Update 是一项 eSupport 技术，它利用本地系统上的更新客户机来传递 Web 上所需的程序包而无需任何用户交互。Active Update 查询并使用可用的更新客户机来安装所需的程序包。Active Update 将在系统上启动 ThinkVantage 系统更新或软件安装程序。

要确定是否已安装 Active Update Launcher，请检查以下注册表键是否存在: HKLM\Software\Thinkvantage\ActiveUpdate

要确定 Active Update Launcher 是否配置为允许 Active Update，HKLM\Software\IBMThinkvantage\Rescue and Recovery 应检查自己的注册表键中 EnableActiveUpdate 属性的值。EnableActiveUpdate=1 将设置“帮助”菜单下的“Active Update”菜单项。

Active Update

要确定是否已安装 Active Update Launcher，请检查以下注册表键是否存在:

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

要确定 TVT.TXT 文件是否配置为允许 Active Update，TVT 应检查自己的注册表键中 EnableActiveUpdate 属性的值。如果 EnableActiveUpdate=1，则 TVT 应在“帮助”菜单下添加“Active Update”菜单项。

要调用 Active Update，调用 TVT 应启动 Active Update Launcher 程序并传递一个参数文件（有关参数文件的描述，请参阅 Active Update 参数文件）。

使用以下步骤来调用 Active Update:

1. 打开 Active Update Launcher 注册表键:

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

2. 获取 Path 属性的值。
3. 获取 Program 属性的值。
4. 连接 Path 属性和 Program 属性中找到的值以构成命令字符串。
5. 将参数文件（请参阅 Active Update 参数文件）追加到命令字符串。
6. 执行命令字符串。以下是生成的命令字符串大致情况的示例:

   ```
   C:\Program Files\ThinkVantage\ActiveUpdate\activeupdate.exe C:\Program
    Files\ThinkVantage\RnR\tvtparms.xml
   ```

建议以异步方式调用 Active Update，这样不会阻止调用 TVT。如果需要在安装更新之前终止调用 TVT，则更新的安装程序应负责终止 TVT。

Active Update 参数文件

Active Update 参数文件包含要传递给 Active Update 的设置。目前只传递 TargetApp（TVT 名称），如下例所示:

```
<root>
       <TargetApp>ACCESSIBM</TargetApp>
</root>
```

```
<root>
       <TargetApp>1EA5A8D5-7E33-11D2-B802-00104B21678D</TargetApp>
</root>
```

附录 D. 管理员工具

ThinkVantage 技术提供可以由公司 IT 管理员调用的工具。

Antidote 向导

有关 Antidote 向导的信息，请参阅第 153 页的附录 F, 『Antidote Delivery Manager 命令参考和示例』。

BMGR CLEAN

CleanMBR 清除主引导记录。当您遇到 Rescue and Recovery 安装故障（例如，由于可用扇区少于安装引导管理器所需的可用扇区而无法安装 Rescue and Recovery）时，可以使用该程序。

注:

1. 运行该工具后，使用 MBR 的应用程序将失效。 例如，SafeGuard Easy、SafeBoot 以及 Computrace 的 MBR 版本等。
2. 应在安装 Rescue and Recovery 之前运行该工具。
3. cleanmbr.exe 适用于 DOS，而 CleanMBR32.exe 则适用于 Windows。
4. 运行 DOS CleanMBR 后，请运行 FDISK /MBR; 它会写入 MBR。

CleanMBR32.exe 的参数为:

表 55.

参数（必选）:	**描述**
/A	清除 MBR 并安装 PC DOS MBR
参数（可选）:	
/Dn	将更改应用到驱动器。对第一个驱动器使用 *n*=0。
/Y	全部是
/?	显示帮助
/H	显示帮助

CLEANDRV.EXE

清除驱动器上的所有文件。运行该命令后，操作系统不再存在。有关更多信息，请参阅第 109 页的『将 Rescue and Recovery 安装到 12 型服务分区中』。

CONVDATE

Convdate 实用程序是作为 Rescue and Recovery 管理工具的一部分提供的。该实用程序用于确定日期和时间的十六进制值并将日期和时间转换为十六进制值，还可以用于设置 TVT.TXT 中备份字段中的定制日期和时间。

```
[Backup0]
StartTimeLow=0xD5D53A20
StartTimeHigh=0x01C51F46
```

要运行该实用程序，请执行以下操作:

1. 从 http://www.lenovo.com/thinkvantage 获取 Rescue and Recovery 管理工具
2. 打开 CMD 窗口
3. 输入 Convdate

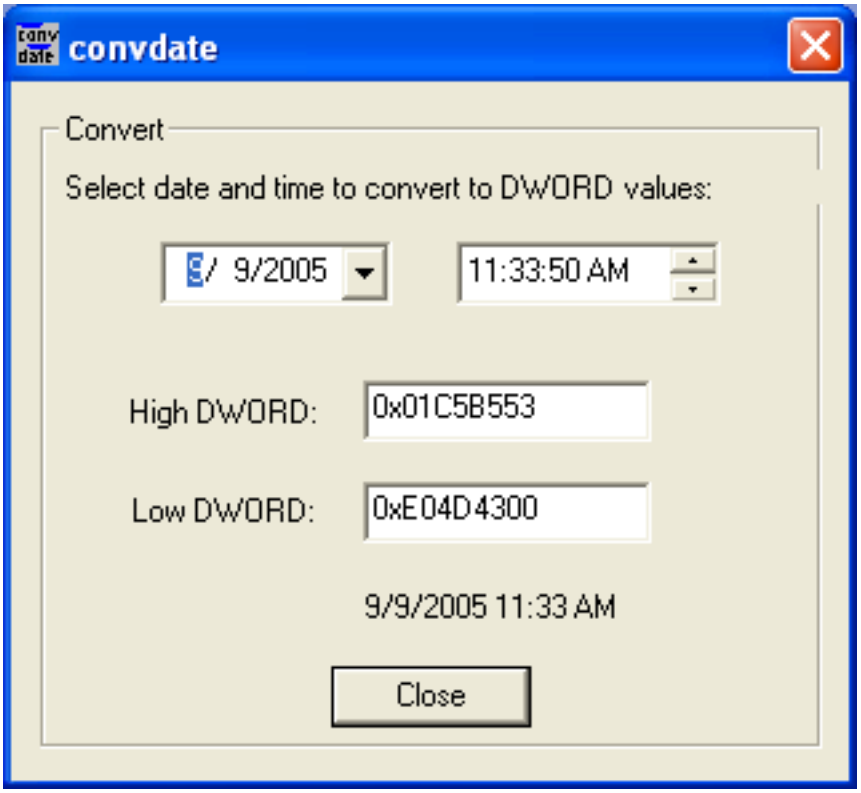

图 5. Convdate 窗口

4. 在 “Select date and time to convert DWORD Values” （选择日期和时间以转换 DWORD 值）字段中输入 “日期和时间”。
5. 相应的 TVT.TXT 文件值为:
   - High DWORD=StartTimeHigh
   - Low Dword=StartTimeLow

CREAT SP

该命令按所需的兆字节为服务分区创建一个分区。盘符是可选的。

语法为:

```
createsp size=x drive=x /y
```

CREAT SP 的参数为:

表 56.

参数	描述
size=*x*	要创建的服务分区的大小（以兆字节为单位）
drive=*x*	创建服务分区的驱动器号。如果不指定，则使用第一个非 USB 驱动器。该参数是可选的。
/y	禁止将清除驱动器的确认。该参数是可选的。

注: bmgr32.exe 必须与 createsp.exe 位于同一目录中并且必须从 WinPE 运行。

RRUTIL.EXE

有关 RRUTIL.EXE 的信息，请参阅第 17 页的『Predesktop Area』。

SP.PQI

该文件可用于创建 12 型服务分区。有关更多信息，请参阅第 109 页的『将 Rescue and Recovery 安装到 12 型服务分区中』。

附录 E. 用户任务

用户可能无法根据用户权限执行某些任务。下表概括了具有受限用户 / 用户、高级用户和管理员缺省操作系统用户标识许可权的基本任务功能。任务和功能因 Windows 操作系统不同而异。

Windows XP

下表显示“受限”、“高级”和“管理”用户可以在 Windows XP 环境中的 Rescue and Recovery 中执行的任务。

表 57. Windows XP 用户任务

Windows XP 用户可以执行以下任务:	**受限用户**	**高级用户**	**管理员**
创建挽救介质 ISO	否	否	是（使用以下提供的命令行）
创建可引导 CD 介质	是	是	是
创建 USB HDD 可引导介质	否	否	是
启动备份	是	是	是
在 Rescue and Recovery 环境（RRE）中初始化复原	是	是	是
在 RRE 中执行单一文件复原	否（Windows） 是（Windows Pre Boot Area）	否（Windows） 是（Windows Pre Boot Area）	是
在 Rescue and Recovery 界面中设置包括和排除	是	是	是
备份到网络驱动器	是	是	是
调度备份	是	是	是

Windows 2000

下表显示“受限”、“高级”和“管理”用户可以在 Windows 2000 环境中的 Rescue and Recovery 中执行的任务。

表 58. Windows 2000 用户任务

Windows 2000 用户可以执行以下任务:	**受限用户**	**高级用户**	**管理员**
创建挽救介质 ISO	否	否	是（使用以下提供的命令行）
创建可引导 CD 介质	是	是	是
创建 USB HDD 可引导介质	否	否	是
启动备份	是	是	是
在 Rescue and Recovery 环境（RRE）中初始化复原	是	是	是

表 58. Windows 2000 用户任务 (续)

Windows 2000 用户可以执行以下任务:	**受限用户**	**高级用户**	**管理员**
在 RRE 中执行单一文件复原	否（Windows） 是（Windows Pre Boot Area）	否	是
在 Rescue and Recovery 界面中设置包括和排除	是	是	是
备份到网络驱动器	否	否	是
调度备份	是	是	是

创建挽救介质

管理员可以使用以下命令行创建挽救介质 ISO。这些命令行将使您能够制作所需的 ISO 文件并且该文件将自动放置到 C:\Program Files\IBM ThinkVantage\Rescue and Recovery\rrcd\ 目录中:

```
:: This 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

 /scripted

:: This 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 /noburn

 /noburn
```

附录 F. Antidote Delivery Manager 命令参考和示例

Antidote Delivery Manager 不仅为管理员提供一个用于创建消息的命令行打包工具，还提供一些在消息中使用的特殊命令功能。

Antidote Delivery Manager 命令指南

引导管理器界面命令行界面是 BMGR32。它驻留在目录 C:\Program Files\IBM ThinkVantage\Rescue and Recovery\ADM 中。下表列出了 BMGR32 的开关及其结果。

表 59. Antidote Delivery Manager 命令

命令	描述
APKGMES [/KEY *keyfile*|/NEWKEY *keyfile*|/NOSIG] *message_directory message_name*	对于 APKGMES /KEY，将根据 *TVT.TXTmessage_directory* 的内容创建一个消息文件。该目录必须包含一个名为 GO.RRS 的文件。如果使用 /KEY 参数，将从 keyfile.prv 检索到一个签署密钥，且 keyfile.pub 中的密钥已分发给将处理该消息的所有客户机。缺省情况下，将使用密钥文件 “KEYFILE.PRV”。/NEWKEY 参数可用于创建密钥。如果不使用签署，则指定 /NOSIG 将阻止签署。将把日期戳记追加到消息名称的末尾，如 *message_name*YYMMDDHHmm.zap。
REBOOT [/*RR*|/Win] [/wait | /f]	该命令重新引导机器。不带任何参数时，以常规引导顺序进行重新引导。参数 RR 表示重新引导至 Rescue and Recovery，参数 WIN 则表示重新引导至常规操作系统。脚本退出后才会进行重新引导，因此这通常应该是脚本中的最后一个命令。可选的 WAIT 命令强制系统在下一次重新引导（手动或由其他机制触发）时引导至指定环境。/f 参数强制系统立即重新引导，并且不允许用户保存来自打开的应用程序的信息。如果未指定任何参数，则程序将 /win 作为缺省参数（不指定 /wait 和 /f）。
RETRYONERROR [ON|OFF] *retries*	缺省情况下，一个脚本只尝试一次。但是，如果一定要不断尝试脚本直至它起作用，则可以使用 RETRYONERROR 命令通知邮箱功能根据 retries 参数指定的有限次数继续尝试执行该脚本。如果未指定任何数字，则缺省值为 3。可以在 TVT.TXT 文件中的 rescue 节中设置一个全局缺省值 retries = *retries*。retries 还可以设置为 FOREVER，它将触发无限循环。

表 59. Antidote Delivery Manager 命令 (续)

命令	描述
MSGBOX /msg *message text* [/head *header_text*] [/OK] [/CANCEL]| [/TIMER *timeout*] /B3	MSGBOX 命令将向已登录的最终用户显示消息。在发生超时、按下“取消”按钮或者按下**确定**按钮（如果指定了 /OK）之前，将保持显示消息并阻止脚本。如果未指定 /CANCEL，则面板上不会显示“取消”按钮，因而难于清除显示内容。命令将返回: • 0 = 按下“确定” • 1 = 取消 • 2 = 计时器到期 可以对消息中的文本进行格式化（分别使用 \n 和 \t 表示新行和制表符）。
NETWK [/D|/E|/A [/IP *ip_address* | /DN *domain_name*] [/NM *netmask*]	NETWK /D（禁用）将通过禁用所有网络适配器来阻止所有网络流量。在运行 NETWK /E（启用）命令之前将禁用联网。NETWK /A 将联网限制到按 /IP 开关（点分十进制）或 /DN（DNS 名称）指定的 IP 地址。/NM 开关提供网络掩码。如果不提供 /NM，则只能访问以 /IP 或 /DN 指定的单台机器。重新引导后仍可以保持该命令的状态，因此必须显式启用联网。
APUBKEY [/ADD|/DELETE] *asn_1_encoded_public_key*	APASSWD 命令使管理员能够远程管理每台 PC 上的 Antidote Delivery Manager 消息签署密钥。每台 PC 上可以存储多个密钥。如果处理签署的消息，将尝试每个密钥直至找到正确的密钥。密钥不是分别命名的，因此必须由内容引用。可以使用 ADD 参数来添加新密钥，并可以使用 DELETE 参数将密钥删除。请注意，如果 TVT.TXT 中指定了任何密钥，则无法再使用未签署的消息（使用 /NOSIG 构建的消息）。
AUNCPW [/Add|/CHANGE|/DELETE] *unc* [/USER *userid*] [/PWD *password*] [/REF *ref_name*]	该命令使您能够为网络驱动器添加、更改或删除密码。引用名称可以用作消息中的快捷方式而不必使用 UNC。返回值为: • 0 = 成功 • 1 = 无法使用提供的信息进行设置 • 2 = 成功，但是已定义一个具有相同引用名称的不同 UNC。

表 59. Antidote Delivery Manager 命令 (续)

命令	描述
XMLtool（条件）	条件（eGatherer，当前硬件信息） • **用法**: xmltool.exe *filename xpath function comparator value* 其中: – **filename** 到 XML 文件的路径和文件名 – **xpath** 到值的标准 xpath – **function** 它必须是以下某个值: - /C，对值进行比较（还必须提供 comparator 和 value） - /F，将指定的值放入 %IBMSHARE%\RET.TXT – **comparator** 必须是以下某个值: - LSS - LEQ - EQU - GTR - GEQ - NEW – **value** XML 条目将与该值进行比较。 • 返回值: – **0** 比较结果为真（/c） – **1** 比较结果为假 – **2** 不正确的命令行参数 – **3** 打开 XML 文件出错（不存在或文件出错） – **4** 指定的 XPATH 未返回值 • **示例**: `xmltool.exe %ibmshare%\\ibmegath.xml //system_summary/bios_version GEQ 1UET36WW`

表 59. Antidote Delivery Manager 命令 (续)

命令	描述
INRR	INRR 命令可用于确定是否正在 Rescue and Recovery 环境中运行脚本。返回值为: • 0 = 当前操作系统 PE • 1 = 当前操作系统不是 PE • >1 = 错误
STATUS [/QUERY *location message_name* | /CLEAR *location*]	STATUS /QUERY 命令可用于确定已运行脚本还是正在排队等待运行。location 值必须是以下某个值: • **FAIL** 消息已运行并且失败 • **SUCCESS** 消息已成功完成 • **WORK** 消息当前正在运行，或者将在下次运行 Antidote Delivery Manager 时运行 • **CACHE** 消息正在排队等待运行 STATUS/CLEAR 命令将清除指定的 *location*。返回值为: • 0 = 如果找到指定的消息或命令成功完成 • 1 = 如果找不到指定的消息或命令失败

受支持的 Microsoft 命令

表 60. 受支持的 Microsoft 命令

命令	描述
ATTRIB.EXE	显示或更改文件属性
CACLS.EXE	显示或修改文件访问控制表（ACL）
CHKDSK.EXE	检查磁盘并显示状态报告
COMP.EXE	比较两个文件或两组文件的内容
COMPACT.EXE	显示或更改 NTFS 分区上的文件压缩
CONVERT.EXE	将 FAT 卷转换为 NTFS。不能转换当前驱动器
DISKPART.EXE	对驱动器进行分区
FC.EXE	比较两个文件或两组文件并显示它们之间的区别
FIND.EXE	在一个或多个文件中搜索某个文本字符串
FINDSTR.EXE	在多个文件中搜索多个字符串
FORMAT.COM	对磁盘进行格式化以用于 Windows
LABEL.EXE	创建、更改或删除磁盘的卷标
NET.EXE	提供联网命令

表 60. 受支持的 Microsoft 命令 (续)

命令	描述
PING.EXE	检查是否可以连接到网络资源
RECOVER.EXE	从出错或受损磁盘恢复可读信息
REG.EXE	注册表操作
REPLACE.EXE	替换文件
RRCMD.EXE	从操作系统运行备份、从操作系统复原或 RR 对输入排序
SORT.EXE	对输入排序
SUBST.EXE	将路径与盘符相关联
XCOPY.EXE	复制文件和目录树

准备和安装

准备

如果将使用签署密钥，管理员需要运行带有 /NEWKEY 参数的打包工具以生成新的签署密钥。

配置

将需要多个配置项。这些项出现在 TVT.TXT 文件中:

存储库

每台客户机都需要存储库列表。这应该包括软盘驱动器、C:\ 以及至少一个使用 UNC 指定的网络驱动器；mailbox = 这是驱动器以及到邮箱位置的路径（按重要性以逗号分隔）。示例:

```
[rescue] mailbox = %y%\antidote, c:\antidote
```

调度信息

调度方式是检查的频率。

表 61. 调度方式

调度方式	
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:\Program Files\IBM ThinkVantage\Rescue and Recovery\adm\mailman.exe
ScheduleHour=11
ScheduleMinute=28
ScheduleDayOfTheWeek=3
ScheduleWakeForBackup=0
```

签署密钥

如果将使用签署密钥，必须将它们分发到客户机。APKGMES 命令创建的文件 keyfile.pub 包含密钥。每个授权的公共签署密钥在 TVT.TXT 文件中显示为: `pubkeyX = ...`（其中 *X* 将替换为一个整数，最多可以存储 9 个公钥）。使用 APUBKEY 函数来设置值 `nosig =`。如果将它设置为 1，则允许运行未签署的程序包（使用 /NOSIG 参数构建的程序包）。

注: 如果不将它设置为 1 或是 TVT.TXT 文件中存在公钥，则不会运行未签署的程序包。

网络驱动器

通过使用 AUNCPW 函数 `RscDrvY` 来设置以下值。每个 `RscDrv` 节包含一个网络共享的相关信息。最多可以为 Antidote Delivery Manager 定义 10 个网络共享。

- UNC = 需要 Antidote Delivery Manager 连接到的驱动器的 UNC。
- User = 加密用户名
- Pwd = 加密密码
- Ref = 要与该连接相关联的引用名称

在客户机上安装

Rescue and Recovery 2.0 必须安装到所有客户机上。可以将以上准备的配置包括在安装中或稍后执行。

服务器基础结构

管理员必须为存储库建立网络共享或是提供 FTP 或 HTTP 站点。可能需要为修订和补丁提供一个附加存储库。

简单系统测试 – 显示通知

脚本准备和打包

在已安装 Antidote Delivery Manager 的任意机器上撰写一个 GO.RRS 脚本。包含以下一行内容: `MSGBOX /MSG "Hello World" /OK`。在命令提示符处直接执行该命令以确保它运行正常。然后，在包含 GO.RRS 的目录中运行 APKGMSG 命令以创建消息。将消息文件放入您机器上的某个存储库目录中并遵循正确的操作。

部署

在部署 Antidote Delivery Manager 之前，应执行以下步骤:

1. 确定邮箱位置:
   - *Mailboxes* 定义为网络共享、HDD 或可移动介质上的本地系统、FTP 或 HTTP 站点上的目录。
   - 您可能发现拥有多个邮箱在无法访问某个邮箱时会有所帮助。最多可以定义十个邮箱位置。
   - 基于网络的邮箱对于客户机应该是只读的并且应该限制写访问权。
2. 在 TXT.TXT 文件中设置邮箱:
   - 在已安装 Rescue and Recovery 的提供者系统上，编辑位于 *C:\Program Files\IBM\ThinkVantage* 目录中的 TVT.TXT 文件。
   - 在 TVT.TXT 文件中创建一个新的 rescue 节。
   - 在 rescue 节中添加以下条目:

     ```
     mailbox=
     ```

     然后添加邮箱目录信息。例如，本地驱动器上的邮箱如下:

     ```
     [rescue]
     mailbox=C:\ADM\Mailbox,
      \\Network\Share
     ```

     FTP 站点上的邮箱如下:

     ```
     ftp://ftp.yourmailbox.com
     ```

     共享网络驱动器上的邮箱如下:

     ```
     \\Network\Share
     ```

     注:

     a. 邮箱功能不支持 HTTPS。

     b. 必须配置 HTTP Web 服务器以提供开启的索引功能和列出文件功能。

     盘符可能在 Windows Professional Edition 与您的常规操作系统环境之间发生变化。C: 盘最可能发生变化。要解决这个问题，请使用环境变量 *CUSTOS*，它始终指向包含典型客户操作系统的驱动器。前面的示例将更改为:

     ```
     mailbox=%CUSTOS%\ADM\Mailbox, ftp://ftp.yourmailbox.com, \\Network\Share
     ```

     只要字符串符合所使用设备或协议的标准，就没有长度限制。例如，如果使用本地文件，则路径不能超出 256 个字符。
   - 多个邮箱条目以逗号或分号分隔。
   - Antidote Delivery Manager 按序在指定的邮箱位置中查找程序包。
3. 如果 FTP 或 HTTP 连接需要用户名和密码，请使用以下格式:

   ```
   ftp//username:password@ftp.yourmailbox.com
   ```
4. 对于网络共享邮箱的用户名和密码:

   用户名和密码条目以加密形式存储在 TVT.TXT 文件中。要在提供者系统上添加条目:

   a. 打开 DOS 窗口

b. 更改目录至 C:\Program Files\IBM ThinkVantage\Rescue and Recovery\ADM

c. 运行以下命令:

```
auncpw /add \\Network\Share /user username /pwd password /ref refID
```

该命令将在 TVT.TXT 文件中创建以下条目:

```
[RscDrv0]
UNC=\\Network\Share
 User=01E23397A54D949427D5AF69BF407D5C
Pwd=04E22197B34D95943ED5A169A0407C5C
Ref=refID
```

注:

a. 可以在 Antidote Delivery Manager 使用的任何系统上使用该条目以获得对同一共享的访问权。

b. Antidote Delivery Manager 最多可以使用 10 个网络共享。

c. 除了 10 个网络共享之外，还可以添加其他邮箱条目（如 FTP 或本地）。

d. AUNCPW.EXE 文件还具有可用于密码管理的其他功能。请在命令行中输入 AUNCPW /? 或参阅第 153 页的表 59。

5. 创建 Antidote Delivery Manager 公钥／私钥对。建议使用 Antidote Delivery Manager 的公钥／私钥对功能。Antidote Delivery Manager 利用公钥／私钥来验证程序包的可靠性。应妥善保存私钥（切勿分发）。通过 Antidote Delivery Manager 管理的每台客户机上都应该有匹配的公钥。要在已安装 Rescue and Recovery 的非提供者系统上创建公钥／私钥对:

a. 打开 DOS 窗口。

b. 向以下目录发出 CD 命令: C:\Program Files\IBM ThinkVantage\Rescue and Recovery\ADM。

c. 运行以下命令:

```
apkgmes.exe /newkey mykey
```

该命令将创建两个文件: mykey.pub 和 mykey.prv（分别是公钥和私钥）。

d. 将公钥复制到提供者系统的 C:\Program Files\IBM ThinkVantage\Rescue and Recovery\ADM 目录中。

e. 使用文本编辑程序（如 notepad.exe）打开文件。

f. 将文件内容复制到剪贴板中。

g. 在命令行中，输入以下命令:

```
apubkey.exe /add x
```

其中 *x* 是剪贴板的内容。

h. 这将在 TVT.TXT 的 [rescue] 节中创建一个条目: pubkey0=906253...。

- TVT.TXT 中最多可以存储 10 个公钥。
- APUBKEY.EXE 文件还具有可用于公钥管理的其他功能。请在命令行中输入 APUBKEY /? 或参阅第 153 页的表 59。

6. 创建 Antidote Delivery Manager 需要在系统上定期运行的调度 Antidote Delivery Manager 检查（允许多个调度）。要设置每 20 分钟运行一次的调度，应将以下内容添加到提供者系统上的 TVT.TXT 文件中:

```
[Scheduler]
Task1=rescuerecovery
Task2=egatherer
Task3=rescue

[rescue]
ScheduleFrequency=0
ScheduleMode=0x01
NumMinutes=20
TaskShow=1
Task=C:\Program Files\IBM ThinkVantage\Rescue and Recovery\ADM\antidote
\mailman.exe
```

其中 *ScheduleMode* 是触发传递 Antidote Delivery Manager 程序包的事件。参数为:

表 62. Antidote Delivery Manager 参数

参数	值
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

注:

a. 调度程序无法在 Pre_Desktop Area 中运行。

b. 有关更多信息，请参阅第 131 页的『调度备份和相关的任务』。

7. 创建 Antidote Delivery Manager 程序包。

   完成上述步骤后，构建并分发您的第一个程序包。在管理员系统（非提供者系统）上，执行以下操作:

   a. 创建一个目录，如 *C:\ADM\Build*。

   b. 在该目录中，创建一个名为 GO.RRS 的文件并添加以下内容:

   ```
   msgbox.exe /msg "Hello World!" /head "test" /ok /cancel
   ```

   c. 保存并关闭该文件。

   d. 向以下目录发出 CD 命令: C:\Program Files\IBM ThinkVantage\Rescue and Recovery\ADM

   e. 运行以下命令:

   ```
   apkgmes.exe /key mykey.prv C:\adm\build HELLOPKG
   ```

   f. 这将创建一个名为 HELLOPKGYY*MMDDHHMM*.ZAP 的程序包,其中 *MMDDHHMM* 将替换为当前日期／时间。

8. 将 HELLOPKGYY*MMDDHHMM*.ZAP 复制到第 2 步中指定的邮箱位置。

9. 调用 Antidote Delivery Manager。

   a. 当提供者系统上的计时器到期时，将运行该程序包并出现 Hello World 消息框。

b. 如果您不希望等待，可以在提供者系统上输入 C:\Program Files\IBM ThinkVantage\Rescue and Recovery\ADM\mailman.exe

示例

以下是 Antidote Delivery Manager 使用方式的一些示例:

示例 1

该示例是一个用于修复由于注册表中的病毒或错误条目而始终显示蓝屏的计算机的程序包。

1. 假定客户机显示蓝屏是由于通过注册表中的 Run Key 执行的病毒所致。要解决这个问题，需要创建一个名为 go.rrs 的文件（它运行 *reg*）。有关 Microsoft 命令的列表，请参阅第 156 页的『受支持的 Microsoft 命令』。Reg 将除去相应的注册表值并从系统中删除相应的可执行文件（如果可能）。它的内容应该如下:

   ```
   reg delete HKLM\Software\Microsoft\Windows\Current Version\Run /v runvirusvalue
   /f del %custos%\windows\system32\virus.exe
   ```

2. 现在将您的 go.rrs 文件放入 *c:\adm\build* 目录中并运行:

   ```
   apkgmes.exe /key mykey.prv C:\adm\build REMOVEVIRUS
   ```

3. 将 REMOVEVIRUS*YYDDHHMM*.ZAP 复制到您的邮箱中。
4. 引导每台客户机并按下 Access IBM 按钮 / F11 或 Enter 键进入 Pre_Desktop Area（其中 mailman.exe 文件在启动时运行），然后运行 REMOVEVIRUS 程序包。

示例 2

该示例向客户机推送 Quick Fix Engineering（快速修复工程）更新或补丁。

1. 创建一个目录用于放置脚本文件和补丁文件（如 *C:\adm\patchbuild*）。
2. 将 qfe 或补丁可执行文件放入 c:\adm\patchbuild 目录中。
3. 创建一个名为 go.rrs 的文件并将以下几行内容放入文件中，但需要定制运行并安装 Microsoft 快速修复工程或补丁的那一行。由于该补丁只能安装在常规的 Windows 操作系统中，所以该脚本可以防止尝试在 Windows Professional Edition 中运行安装。

   ```
   set custos
   if errorlevel 1 set custos=%systemDrive%
   %custos%\Program Files\IBM ThinkVantage\Rescue and Recovery\ADM\retryonerror
   /on 10
   %custos%\Program Files\IBM ThinkVantage\Rescue and Recovery\ADM\InRR.exe
   if errorlevel 2 goto ERROR
   if errorlevel 1 goto InOS
   if errorlevel 0 goto InPE

   :ERROR
   exit 1

   :InOS
   REM DISABLE NETWORKING
   Netwk.exe /d
   patchinstall.exe
   REM ENABLE NETWORKING
   Netwk.exe /e
   msgbox.exe /msg "Patch Installed" /head "Done" /ok
   exit 0

   :InPE
   exit 1
   ```

4. 将 go.rrs 放入 c:\adm\patchbuild 目录中并运行:

```
apkgmes.exe /key mykey.prv C:\adm\patchbuild PATCHBUILD
```

5. 将 PATCHBUILD*YYDDHHMM*.ZAP 复制到您的邮箱中。
6. 客户机下一次调度运行 mailman.exe 文件或重新引导客户机时将安装补丁。

检查程序包是否已完成的方法

- **Fail.log**

  该文件通常存储在 *c:\ibmtools\utils\rescue* 目录中。如果存在包含任何非零值的 zap 文件，将把它记录到该文件中。

- **Rescue.log**

  该文件通常位于 *c:\ibmshare* 目录中。该文件提供更详细的信息，这些信息可以帮助您确定程序包的失败原因或确保程序包运行正常。它在 zap 文件中逐行记录发生的事件。

- **Success.log**

  该文件通常存储在 *c:\ibmtools\utils\rescue* 目录中。如果包含零值的 zap 文件退出，将把它记录到该文件中。

示例 3

该示例在 Pre_Desktop Area 中使用 FTP 或 HTTP 站点:

1. 为程序包定义一个外部 Web 站点:

   ```
   ftp.yourmailbox.com
   ```

2. 创建公钥／私钥（请参阅第 5 步）。
3. 将邮箱添加到 TVT.TXT 中:

   ```
   mailbox=ftp://username:password@ftp.yourmailbox.com
   ```

4. 当用户按下 Access IBM／F11 或 Enter 键进入 PreDesktopArea 时，Antidote Delivery Manager 程序包会在引导时于 Pre_Desktop Area 中执行。

示例 4

该示例使用 xmltool.exe 文件来定位特定客户机:

1. 分发 xml 文件，该文件中包含要通过 Active Directory、Systems Management Server 或其他管理工具与客户机进行比较的信息。

   ```
   <file>
   <activedirgroup>Marketing</activedirgroup>
   </file>
   ```

2. 在 go.rrs 文件的第一行中，放置一个使用 xml 工具的行。该行是一个“只”定位营销组中的机器的示例:

   ```
   xmltool.exe c:\mycompany\target.xml //file/activedirgroup /c EQU Marketing
   if errorlevel 0 goto RUNIT
   exit errorlevel

   :RUNIT
   #place code to execute patch or whatever action
   ```

主要蠕虫程序攻击

以下示例演示了抵御主要病毒的一种可行方法。基本方法是关闭联网、然后重新引导至 Rescue and Recovery、修复注册表、将替换文件复制到位，然后引导回 Windows XP 并复原联网。为了进行演示，需要更新以下应用程序以修改语法。

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 "System will reboot in 20 seconds \n  \n Press OK to reboot now, or Cancel to
reboot later."
/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.
```

附录 G. 声明

Lenovo 可能不在所有国家或地区提供本文档中讨论的产品、服务或功能特性。有关您当前所在区域的产品和服务的信息，请向您当地的 Lenovo 代表咨询。任何对 Lenovo 产品、程序或服务的引用并非意在明示或暗示只能使用 Lenovo 的产品、程序或服务。只要不侵犯 Lenovo 的知识产权，任何同等功能的产品、程序或服务，都可以代替 Lenovo 产品、程序或服务。但是，评估和验证任何其他产品、程序或服务，则由用户自行负责。

Lenovo 公司可能已拥有或正在申请与本文档内容有关的各项专利。提供本文档并未授予用户使用这些专利的任何许可。您可以用书面方式将许可查询寄往:

Lenovo (United States), Inc
500 Park Offices Drive, Hwy 54
Research Triangle Park, NC 27709
USA
Attention: Lenovo Director of Licensing

LENOVO GROUP LTD. “按现状” 提供本出版物，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的有关非侵权、适销或适用于某种特定用途的保证。某些管辖区域在某些交易中不允许免除明示或暗含的保证，因此本条款可能不适用于您。

本信息中可能包含技术方面不够准确的地方或印刷错误。此处的信息将定期更改；这些更改将编入本出版物的新版本中。Lenovo 可以随时对本出版物中描述的产品和／或程序进行改进和／或更改，而不另行通知。

本文档描述的产品并非旨在用于移植或其他生命支持的应用，在这些应用中的故障可能导致人身伤害或死亡。本文档中包含的信息不影响或更改 Lenovo 产品规格或保证。根据 Lenovo 或第三方的知识产权，本文档中的任何内容都不能作为明示或暗含的许可或保证。本文档中包含的所有信息都在特定的环境下获得并且作为说明提供。在其他操作环境中获得的结果可能不同。

Lenovo 可以按它认为适当的任何方式使用或分发您所提供的任何信息而无须对您承担任何责任。

本出版物中对非 Lenovo Web 站点的任何引用都只是为了方便起见才提供的，不以任何方式充当对那些 Web 站点的保证。那些 Web 站点中的资料不是 Lenovo 产品资料的一部分，使用那些 Web 站点带来的风险将由您自行承担。

此处所包含的任何性能数据都是在受控环境中测得的。因此，其他操作环境中的结果可能会有明显的不同。有些测量可能是在开发级的系统上进行的，因此不保证这些测量与在一般可用系统上进行的测量结果相同。此外，有些测量可能是通过推算估计出的。实际结果可能会有不同。本文档的用户应该验证其特定环境下的适用数据。

商标

下列术语是 Lenovo 在美国和／或其他国家或地区的商标:

Lenovo
Rescue and Recovery
ThinkPad
ThinkCentre
ThinkVantage
Rapid Restore

Intel 是 Intel Corporation 或其子公司在美国和其他国家或地区的商标或注册商标。

下列术语是 International Business Machines Corporation 在美国和／或其他国家或地区的商标: IBM、Lotus® 和 Lotus Notes

Microsoft、Windows 和 Windows NT® 是 Microsoft Corporation 在美国和／或其他国家或地区的商标。

其他公司、产品和服务名称可能是其他公司的商标或服务标记。

词汇表

〔C〕

存储根密钥（Storage Root Key，SRK）： 存储根密钥是一个 2,048 位（或更大的）公钥对。它最初是空的并在分配 TPM 所有者时得以创建。这个密钥对始终不离开嵌入式安全芯片。它用于对可信平台模块之外的存储的私钥进行加密（打包）并在这些私钥装回可信平台模块时对它们进行解密。能访问 BIOS 的任何人员都可以清除 SRK。

〔D〕

对称密钥加密（Symmetric-key encryption）： 对称密钥加密密码对数据加密和数据解密使用相同的密钥。对称密钥密码更简单并且速度更快，但它们的主要缺点是双方必须设法安全地交换密钥。公钥加密则可以避免这个问题，因为公钥可以通过非安全方式分发，而私钥则始终不必传送。高级加密标准是对称密钥的一个典范。

〔G〕

高级加密标准（Advanced Encryption Standard，AES）： *高级加密标准*是一种*对称密钥*加密技术。美国政府于 2000 年 10 月采用该算法为其加密技术，用以取代以前使用的 DES 加密。AES 针对蛮力攻击（brute-force attack）提供的安全性比 56 位 DES 密钥更强，并且 AES 还可以根据需要使用 128 位、192 位和 256 位密钥。

公钥／对称密钥加密（Public-key/Asymmetric-key encryption）： 公钥算法通常使用一对相关密钥 – 其中一个密钥是私钥并且必须保密，另一个密钥则可以公开并广泛分发；不能由给出的密钥推断出同对密钥中的另一个密钥。术语“公钥加密”源自以下构思 – 使部分密钥成为公共信息。同时也使用术语“对称密钥加密”，因为并非各方都持有相同的信息。在某种意义上，一个密钥将锁“锁定”（加密）；而将该锁“解锁”（解密）则需要另一个密钥。

管理员（ThinkCentre）／超级用户（ThinkPad）BIOS 密码: 管理员或超级用户密码用于控制更改 BIOS 设置的能力。这包括启用／禁用嵌入式安全芯片以及清除可信平台模块（Trusted Platform Module）中存储的存储根密钥（Storage Root Key）的能力。

〔J〕

加密系统（Cryptography system）： 加密系统可以大致分为对称密钥加密和公钥加密，前者使用一个密钥对数据进行加密和解密，后者则使用两个密钥（每个人都知道公钥并且只有密钥对的所有者才能访问私钥）。

〔K〕

可信平台模块（Trusted Platform Module，TPM）： 可信平台模块植入系统中的专用集成电路，它可以实现强大的用户认证和机器验证。TPM 的主要目的是防御对机密信息及敏感信息的不当访问。TPM 是基于硬件的信任根，可用于为系统提供各种加密服务。TPM 又称为嵌入式安全芯片。

〔Q〕

嵌入式安全芯片（Embedded Security Chip）： 可信平台模块（Trusted Platform Module）又称为嵌入式安全芯片。

ThinkVantage

部件号: 41R9862

中国印刷

(1P) P/N: 41R9862