

Realtime  
publishers

"Leading the Conversation"

*The Definitive Guide™ To*

# Vista Migration

*sponsored by*



altiris®

*Danielle Ruest  
and Nelson Ruest*

Chapter 7: Kernel Image Management .....	173
Defining the Logical OS Configuration.....	175
Physical Layer.....	176
Operating System Layer .....	177
Networking Layer .....	177
Storage Layer .....	178
Security Layer.....	179
Communications Layer.....	181
Common Productivity Tools Layer .....	182
Presentation Layer .....	183
Non-Kernel Layers.....	184
Identifying Kernel Contents.....	184
“Thick” versus “Thin” Images.....	185
Using a Single Worldwide Image.....	187
Discovering the Installation Process.....	188
Identifying Hardware Requirements.....	188
Identifying Installation Methods.....	189
Using Installation Documentation .....	194
The Installation Preparation Checklist.....	195
Documenting PC Installations .....	196
Post-Installation Processes.....	196
Supported Installation Methods .....	198
Selecting an Installation Process.....	199
Determining the Physical OS Configuration .....	199
Applying the Post-Installation Checklist .....	200
Update the Default User Profile.....	203
Determining the OS Deployment Method .....	205
Preparation and Prerequisites.....	207
Build a Smart Solution.....	208

## Copyright Statement

© 2007 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.com, Inc. (the “Materials”) and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimepublishers.com and the Realtimepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at [info@realtimepublishers.com](mailto:info@realtimepublishers.com).

[**Editor's Note:** This eBook was downloaded from Realtime Nexus—The Digital Library. All leading technology guides from Realtimepublishers can be found at <http://nexus.realtimepublishers.com>.]

## Chapter 7: Kernel Image Management

Each time you perform a PC operating system (OS) deployment, you need to figure out how the installation will proceed. For this, you must discover exactly how the OS installation process works and then, you determine how you can automate the process. With Vista, Microsoft has introduced a completely new installation process called Image-based Setup (IBS). Basically, each version of Windows Vista includes a system image file—called a .WIM file—that contains the installation logic for different editions of Vista. During the IBS installation process, this system image file is copied to the system disk and then expanded and customized based on the hardware that is discovered during the process.

WIM images contain several different editions of Vista. Common files are not duplicated within the WIM as it relies on a single instance store (SIS) to include only one copy of each common file as well as individual copies of the additional files that build different editions. The edition you install is determined by the product key you insert during installation. This lets Microsoft ship every edition of Vista on a single DVD. Of course, two system images are required: one for 32-bit and one for 64-bit systems as the architecture for the x86 or the x64 version is incompatible with the other and cannot be contained within the same image. Despite this, having to manage two DVD versions of Vista is a vast improvement over previous versions of Windows where each edition was contained in a different CD or DVD. Of course, you'll have to use a preparation process to create these images (see Figure 7.1).

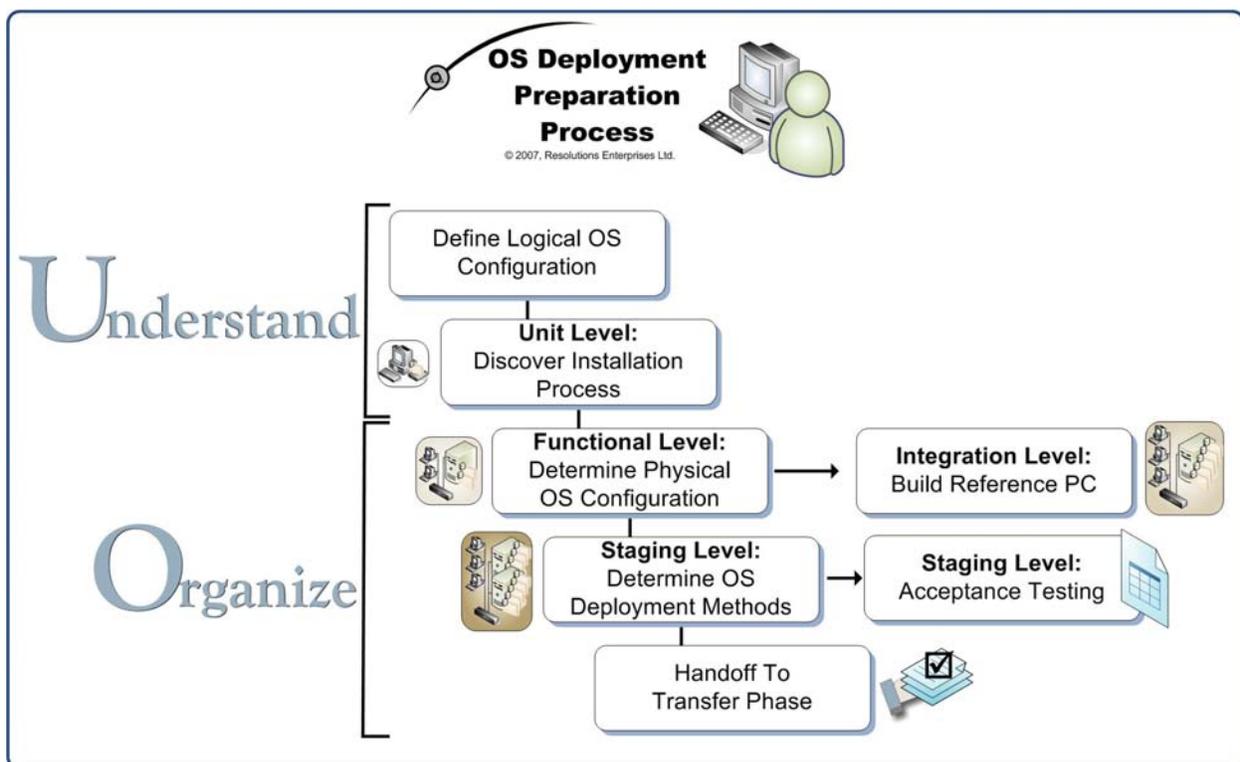


Figure 7.1. The OS Deployment Preparation Process

The preparation process for OS deployment involves several steps which include:

- Defining the Logical OS Configuration
- Discovering the Installation Process
- Determining the Physical OS Configuration
- Determining the OS Deployment Methods

This is the focus of the PC Image Development portion of your deployment project or the Desktop Deployment Lifecycle (see Figure 7.2). Once again, the focus of these activities is the PC Team and the bulk of the work will be performed in the Organize phase of the QUOTE system. But, as in other processes, some activities must be performed in previous phases. For example, the Logical OS Configuration is usually defined during the Understand phase of the QUOTE as is the discovery of the installation process. And, as is the case with all other engineering aspects of the solution you are preparing, the prepared system image and deployment process you select must go through a final acceptance process before it can move on to other phases of the QUOTE and be deployed through your network.

Each of these activities and their related duties are discussed in detail through this chapter. And, as discussed in Chapter 6, the focus of this chapter is to create a system image which will support both application virtualization and standard software installations though you should aim to move to application virtualization since it provides a completely new way of managing applications and maintaining stability within deployed PCs. Virtualization protects the OS at all times and provides significant cost reductions for managed systems.

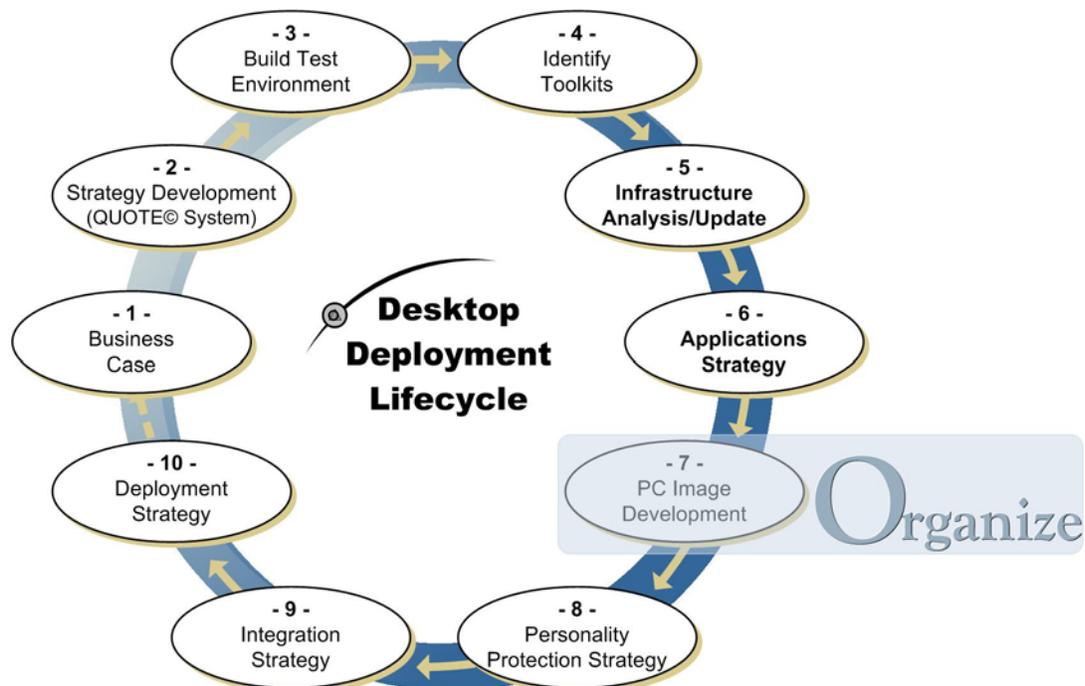


Figure 7.2. Moving through Step 7 of the DDL

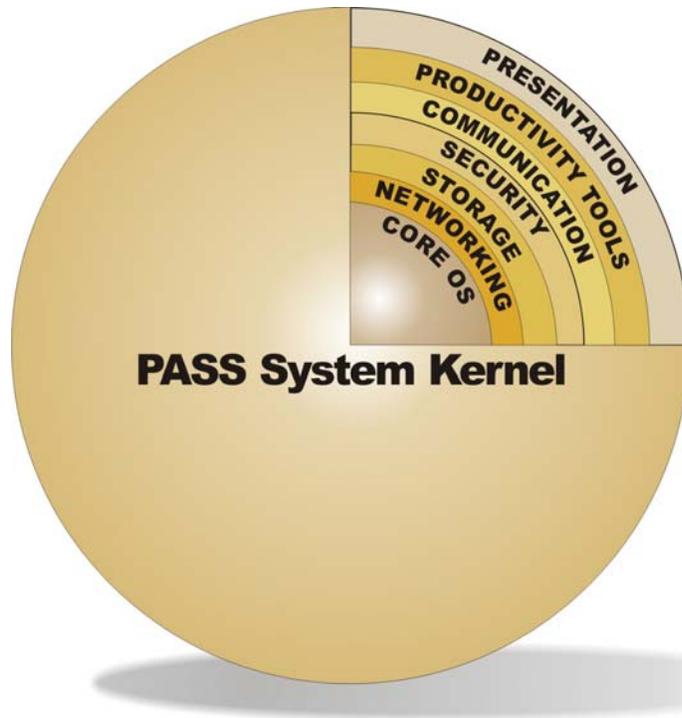
## Defining the Logical OS Configuration

 This activity is part of the **Understand** phase of the QUOTE system.

Designing a computer system for end users is more than just a technical task. After all, end users will be working with the design IT produces every working day. Remember that the goal of end users is to produce work related to the organization's business goals, not to work with or troubleshoot computer systems. With that in mind, IT needs to consider exactly how it can configure a PC operating system to provide the fullest and most user-friendly support for the work they do. To do this, IT must have a sound understanding of the business their organization is in and must design the structure of the OS to be deployed with this business architecture in mind; thus, the need for a logical OS configuration and design.

 For information on how business architectures drive IT services, see the Architectures article series at <http://www.reso-net.com/articles.asp?m=8>. This set of seven articles was designed to assist organizations and IT professionals understand the different cogs that make up enterprise architectures.

Chapter 6 introduced the concept of a system stack: the PASS model. This model lays out the logical organization of deployed components on a PC. While chapter 6 focuses on the application-specific layers of this system stack, this chapter focuses on the components that make up the system kernel—or the elements that are deployed on every single PC in your network (see Figure 7.3).



*Figure 7.3. The Seven Components of the PASS System Kernel*

In addition to the seven layers of the kernel, the PC team responsible for system image creation and deployment will need to be involved with the physical layer. That is, they need to participate in the creation of your baseline computer systems for the Vista operating system. The content and the implications of each of the kernel layers as well as the physical layer are discussed below.

### **Physical Layer**

The physical layer covers PCs, laptops, tablet PCs, cabling, printers, scanners and all other physical components of the PC infrastructure. Standards should be set for baseline systems. Each model you elect to support should conform to these minimal standards. The breadth of this layer for should cover:

- Processor and speed.
- RAM capacity and minimum RAM requirements.
- Drive bay capability, minimum hard disk storage as well as minimum required amount of free disk space.
- Networking components.
- Power management (ACPI).
- Video capability.
- Additional input and output components (CD/DVD readers and writers, keyboard, mouse, USB and Firewire ports, and so on).
- Security components such as Trusted Protection Modules (TPM), biometric or smart card authentication devices and processor-embedded antiviral capabilities.

Ideally, all the hardware you will purchase will be based on industry standards such as those proposed by the Distributed Management Task Force (<http://www.dmtf.org/home>). One of the great standards to emerge from the DMTF is the ability to remotely deploy hardware-specific components such as the computer basic input/output system (BIOS) and other firmware. Make sure you select systems that support this ability and that your provider either delivers its own tool for firmware management or delivers firmware upgrades that are deployable through systems management tools.

## Operating System Layer

The operating system layer focuses on the components that make the OS run on a system. This means:

- The Windows OS, in this case, Vista, but also which editions of Vista you choose to support.
- Appropriate levels of service pack and/or hot fixes; ideally, these are included in the system image you deploy.
- Manufacturer-certified drivers for all peripheral equipment. Certified drivers are a key component of your roll-out. Driver signing is configured through Group Policy. If you can, you should aim to use only certified drivers on all hardware because they are proven to work with Vista. If you need to include non-certified drivers make sure you test them fully.
- The dynamic link libraries (DLL) required in support of organizational applications. For example, this could include runtime versions of libraries such as Visual Basic, Microsoft Access, and any other engine that is required to run your applications on client PCs.
- Organization-wide operating system complements such as typefaces or fonts, regional settings, perhaps language packs if they are required and so on.

Make this layer as complete as possible. For example, if this layer includes the Access runtime, then you will not need to deploy the full version of Access to people who only make use of Access applications and do not develop them.

## Networking Layer

The networking layer covers all of the components that tie the network together including:

- Unique networking protocol: This should be TCP/IPv4 and/or IPv6.
- Networking agents: Any agent or driver that is required to let the PC communicate over local area or wide area networks as well as wireless networks or Bluetooth devices.
- LDAP directory structures: For Windows networks, this means a standard Active Directory structure for all domains, groups and organizational units—this controls what users “see” when they browse the network.
- Unique object naming structure: Every network object—PCs, servers, printers, file shares—should have a unique and standard naming structure.
- Unique scripting approach: Every script should be unified and should be based on a single scripting language. Ideally, scripts should be digitally signed and should be tied to Windows’ Software Restriction Policies so that only authorized scripts can be executed in the network.

- Legacy system access: A unique set of components should be used to access legacy systems such as mainframe computers.
- Remote access and virtual private networking (VPN): This layer should include the components for either remote access or VPN access to the corporate network and any other external system required by users.
- Remote object management: Every component required on PCs for remote management and administration should be part of this layer since the network is what ties the distributed system together. With the advent of Active Directory and the control it offers over PCs, this now includes the Group Policy processing agent which is part of Windows by default. This should also include agents for PC management such as those provided by your deployment mechanism or even BIOS or firmware distribution agents.

Basically, the networking layer includes every component that lets you communicate with the PC and lets the PC communicate with the external world.

### **Storage Layer**

The storage layer deals with the way users interact with both local and remote storage. It covers:

- Physical components: Disk sub-systems, network storage systems, backup technologies.
- Storage software: The systems that must administer and manage storage elements. In some cases, you may need to use third party tools in support of custom storage requirements. A good example is custom DVD burning software.
- File services: File shares, for Windows this also means Distributed File Services (DFS), a technology that integrates all file shares into a single unified naming structure making it easier for users to locate data on the network. DFS also includes replication technology to provide fault-tolerance in a distributed environment.
- Indexing & Search services: All data must be indexed and searchable. For Windows Server 2003, this refers to the Indexing service. For Vista and Longhorn Server, this refers to the integrated Search service.
- Databases: Since data has many forms, the storage layer must support its storage in any form. Structured and unstructured.
- Transaction services: This layer should control transaction services because these services validate all data stored within databases.
- Data recovery practices and technologies: All data must be protected and recoverable. The Vista OS includes both Volume Shadow Copies and the Previous Versions client. This lets users recover their own files. These tools should be integrated to your overall backup and data protection strategy.
- File structure: The file structure of all storage deposits, local (on the PC) and networked, must use a single unified structure. This structure should support the storage of both data and applications.

- **Data replication technologies:** Data that is stored locally on a PC to enhance the speed of data access should be replicated to a central location for backup and recovery purposes. For Windows Server, this means putting in place an offline storage strategy and relying on folder redirection to protect data that is local to the PC.
- **Temporary data storage:** The PC disk drive should be used as a cache for temporary data storage in order to speed PC performance. This integrates with the offline caching strategy.
- **Single unified tree structure:** All PC disk drives should have one single unified tree structure so that users do not have to relearn it. In addition, all PC management tools should be stored as sub-directories of a single, hidden directory. Users should not have access to this folder. In addition, you may need to incorporate a special local folder structure for unprotected data—data that belongs to users only and that the organization is not responsible for.

The objective of the storage layer is to simplify data access for all users. If all structures are unified, then it becomes really easy for all users, especially new users, to learn.

### **Security Layer**

The security layer includes a variety of elements, all oriented towards the protection of the organizational business assets:

- **Ownership of IT assets:** The first part of a security strategy is the outline of ownership levels within the IT infrastructure. If a person is the owner of a PC, they are responsible for it in any way they deem fit. But if the organization is the owner of an asset, people must follow unified rules and guidelines concerning security. This should be the first tenet of the security policy: every asset belongs to the organization, not individuals.
- **User profiles:** Each user has a personal profile that can be stored centrally if possible. This central profile can be distributed to any PC used by the person. Ideally, this is performed through folder redirection Group Policies instead of roaming profiles. Roaming profiles are an outdated technology that put a strain on network communications. Folder redirection link with offline caching to better control bandwidth utilization. Profiles are part of the security layer because by default, each profile is restricted to the person who owns it. Security strategies must support this exclusive protection.
- **Group Policy:** Group Policies, both local and remote, allow the unification and enforcement of security approaches within a distributed environment. By applying security through policies, IT departments ensure that settings are the same for any given set of users.
- **Access rights and privileges:** Each individual user should be given specific and documented access rights and privileges. Wherever possible, access rights and privileges should be controlled through the use of groups and not through individual accounts.
- **Centralized access management:** Security parameters for the corporate IT system should be managed centrally through unified interfaces as much as possible. Local security policies are available but they should be stored centrally and assigned to each PC.

- Non-repudiation technologies: Every user of the system should be clearly identifiable at all times and through every transaction. For Windows, this means implementing using specific, named accounts—not generic—for each user in the organization. For true non-repudiation, a Public Key Infrastructure should be implemented for the distribution of personal certificates which can then be used in emails, documents and other data signed by the individual.

 For more information on the use of PKI in organizations of all sizes, see **Advanced Public Key Infrastructures** at <http://www.reso-net.com/articles.asp?m=8>.

- Internal and external access control: Access to the organizational network should be controlled at all times. This should include every technology that can assist this control such as firewall agents, smart cards, biometric recognition devices, and so on. For Internet access control with Windows, this can mean implementing Microsoft Internet Security and Acceleration Server (ISA) with Whale technologies.

 For more information on the use of ISA Server in organizations of all sizes, see <http://www.microsoft.com/isaserver/default.mspx>.

- Confidential storage: Since PCs, especially mobile systems, are not permanently tied to the network, it is important to ensure the confidentiality of any data stored locally. With Windows Vista, this means implementing either the Encryption File System (EFS) or BitLocker.

Security is at the heart of every IT strategy. This is why this layer is so important and so all-encompassing. Make sure your security policy is public and properly broadcasted to every user in your organization. If you have outsourced personnel, make sure the security policy is one of the first elements they are presented with when they come to work in your organization.

## Communications Layer

The communications layer deals with elements that support communication in all of its forms:

- Instant and deferred communications: These technologies include a variety of electronic communications tools such as electronic mail, instant messaging, discussion groups, IP telephony, video communications, and more. Ideally, you will provide a unified communications strategy to users.
- Workflow and collaboration: Workflow and collaboration is an essential form of online communication today. Your IT infrastructure should support this powerful mechanism. In Windows, this usually involves either the free Windows SharePoint Services (WSS) or Microsoft Office SharePoint Server (MOSS).

 More information on WSS can be found at <http://www.microsoft.com/technet/windowsserver/sharepoint/default.aspx>. Information on MOSS is at <http://office.microsoft.com/en-us/sharepointserver/FX100492001033.aspx>.

- Shared conferencing: Virtual conferencing is a tool that should be available to users to reduce physical meeting costs. More and more providers offer this kind of technology. IT will have to choose whether these sessions are hosted internally or through external Web Services.
- Internet browser: The browser is an essential part of any communications strategy. It must be customized to organizational standards and must be run in protected mode as much as possible.
- Broadcast technology: IT, the organization and individual departments must have a means of communicating vital and timely information to their respective users. This requires some form of broadcast technology. This can be in the form of Windows Media Services or through simple means such as network message broadcasts. In Vista, this can be done through Really Simple Syndication (RSS) feeds delivered to Gadgets displayed on the desktop.
- Group and individual agenda scheduling: Since time management often incurs a communication process, the network infrastructure should support agenda scheduling at both the individual and the group level. This should also include the ability to schedule objects such as meeting rooms, video projectors, and so on.
- Legacy system access: If Terminal Emulation is a requirement; this should include a single unified Terminal Emulator application. Ideally, this will be integrated to the selected browser technology.

Communications is essential to make the organization work. After all, users must communicate with each other and with external resources to perform their work. It is responsible to ensure that these communications are facilitated as much as possible and secure at all times.

### **Common Productivity Tools Layer**

Since most office workers need to rely on productivity tools to perform their work, this layer is an essential part of the core system image you will be deploying to all users. It should include both common commercial tools as well as any organization-wide internally-developed tools required by your organization.

- **Information production tools:** Office automation tools such as Microsoft Office should be available to every user that requires its use. Most commonly, these are deployed to every single user. But, these tools should be deployed intelligently. If users do not require specific components of the suite, then these components should not be deployed to them. For example, most users will require Word, Excel, PowerPoint and Outlook, but not necessarily require the other components of the suite. Deploy only what is required.
- **Generic graphics tools:** All users should be able to illustrate concepts and create drawings. Illustration is a basic communications tool; it must be part of a core set of PC tools. The office automation suite you deploy includes these basic illustration tools. But, you may also need to deploy graphics file viewers such as the Microsoft Visio viewer to let users view illustration produced by more professional illustrators in your organization. This also means implementing server-based technologies that allow the indexing and sharing of illustrations. In some cases, this will mean integrating custom filters to the Indexing service.
- **Service packs:** Common tools should be regularly updated as service packs and hotfixes are released for them.
- **Lexicons and vocabularies:** Lexicons and corporate vocabularies should be unified to ensure the consistency of all output.
- **Commercial utilities:** Common commercial utilities such as Adobe Acrobat Reader, file compression and search engines should be included here. Vista already includes many of these, including a new XPS document writer and reader.
- **Corporate or organizational applications:** Organizational tools such as time sheets, expense reports or even enterprise resource planning clients should be included in this layer.

The goal of this layer is to ensure that every tool that is required by the entire user base is made available to them. The objective of the kernel is to provide a fully functional PC system to users. If this layer is designed properly, it will often satisfy the requirements of a majority of your user base.

## Presentation Layer

The presentation layer is the interface layer. For users, it most often means the design of the organizational desktop. One of the advantages of Microsoft Windows is that its design is entirely based on one principle: common user access (CUA) guidelines. This is a defined set of rules that outlay how people interact with PCs. CUA defines menu interfaces, keyboard shortcuts, and mouse movements and sets standards for their method of operation.

For example, users who are familiar with Microsoft Word, have since its inception in the early 1980s, used the same set of keyboard shortcuts. None of these users has had to relearn any major keystroke since it first became popular and these keystrokes still work today. Good user interfaces are designed to make it easy to transfer from one version of an application to another. Of course, Vista and Microsoft Office 2007 both offer new interfaces, but since they are still based on the CUA, they are relatively easy to learn.

 You can browse articles on the subject of user interface design at <http://msdn2.microsoft.com/en-us/library/aa286531.aspx>.

The advantage of Microsoft's approach is that there is a standard interaction mode within Windows' own presentation layer, but organizations should move beyond the default Windows desktop and specifically enhance Windows' defaults with their own desktop design. This custom design should include:

- Desktop design: The desktop should offer a single unified design to all users. All users should be familiar with this design because it is the default design activated at any new logon within the network. This design should be divided into specific desktop zones that contain different information.
- Local versus central desktop control: Users should be aware of the elements they are allowed to modify on the desktop and which items are locked from modifications.
- Common shortcuts: Every basic shortcut on the desktop should be the same on all systems. Users can add their own, but should not be able to remove the most common shortcuts.
- Common menus and Quick Launch Areas: Tool access should be standardized and all menu sub-categories should be reduced as much as possible. When applications install, they tend to install a series of extraneous shortcuts such as "Visit our Web Site for Free Offers". These are not required within the organizational networks.

The focus of this layer is to introduce a common desktop for all users. Some areas of this desktop are locked so that users in your organization can quickly find what they need on any PC. Others are open so that users can personalize desktops to some degree. Vista includes a host of features that are now controllable by standard users and were not available in previous versions of Windows. This facilitates the design of the PC's presentation layer.

 The key to the construction of a common presentation layer for all systems is the update of the Default User Profile on the Reference PC before capturing its content into a system image that will be deployed to all systems.

## **Non-Kernel Layers**

Chapter 6 discussed the non-kernel layers extensively. These layers are created over and above the kernel and are designed to address specialized as opposed to generalized user needs. Ideally, you will be able to group the IT roles your specialized users play to deliver non-kernel applications in groups. Structuring your PC construction or system stack in this manner lets you reduce system construction costs because of the following benefits:

- Specialized applications are grouped into IT roles. This means they will coexist on a system with a smaller group of applications, including the applications hosted by the kernel. If you are using traditional application installation methods, then this reduces the possibility of conflicts.
- Since applications are grouped into IT roles, they are easier to track. An IT role automatically incurs the cost of the specialized applications it contains, thus departments and other groups within your organization can be charged for these applications. Kernel applications usually have organization-wide licenses so they are also easy to track.
- Since applications are grouped into IT roles, they can be delivered as a group and removed as a group should the primary function or user of a PC change.
- And, if you are using application virtualization as suggested in Chapter 6, you can easily deliver applications in groups, activating them or deactivating them from target PCs through simple mechanisms such as Active Directory (AD) security group membership.

Overall, the PASS system stack provides a structured approach to PC construction and long-term management. This layered approach to IT services provides a simpler model to follow than the traditional ad hoc approach because it relies on familiar imagery. Graphically, the PASS kernel represents a design that is very similar to the OSI Reference Model. This model begins to demonstrate how we can construct and present IT systems in an understandable manner.

## **Identifying Kernel Contents**

The makeup of your own Kernel will depend entirely upon the needs of your organization, but what you need to do at this stage is to run through the different functions and operations of your organization to determine how you can best support it with a system kernel. Some choices are obvious—everyone needs antivirus, anti-spam, antispyware tools and most everyone needs a productivity suite such as Microsoft Office—while others are a bit more complex, mostly because they are particular to your own organization.

Ideally, you would create a data sheet listing each of the seven layers of the PASS kernel and identify the contents of each. Then, when you're satisfied with your selections and have received acceptance and approval on the structure of your new kernel, you can proceed to the next phases of system image preparation.

You might also add the physical layer to this data sheet as it will be important to keep the contents of this layer in line with the expected performance levels your systems will provide when running Windows Vista. More on the contents of this layer will be discussed as you prepare the physical solution that matches the logical solution you just created.

Additionally, you will need to keep two other factors in mind as you prepare to construct your system kernel. The first deals with actual image content: will you be using a ‘thick’ or a ‘thin’ system image? The second mostly concerns global organizations or any organization that has employees who work in different languages. Will you build a single worldwide image or will you create more than one image. The more images you create, the more your maintenance costs will be.

 PCs should be acquired both centrally and in lots as much as possible. Organizations that allow departments to purchase their own PCs are only asking for increased headaches when it comes to PC management. When departments are allowed to purchase their own PCs, there are no standard configurations or even standard suppliers. Diversity is NOT a good thing when it comes to PC management within an enterprise. You should always strive to limit the number of suppliers you purchase from as well as limiting the types of PCs you purchase from these suppliers. Even with these standards in place, you’ll find that the same manufacturer will ship the same PC with different components depending on the ship date. But at least, if you implement purchasing standards for PCs, you will have some measure of control over what you will be managing and you will be able to simplify your OS deployments.

### “Thick” versus “Thin” Images

While it is important that you include all of the proper content into the logical design of your system kernel, you also have to decide whether your physical system image will be thick or thin. Traditionally, organizations have been relying on thick or fat images. It makes sense in a way. Fat images contain everything that should be within the system kernel. Since the preferred deployment method for operating systems is the disk image or system image—a copy of the contents of a reference computer prepared through custom processes and to be duplicated on any number of PCs—it makes sense to make this image as complete as possible. Then, through the use of technologies such as multicasting—the ability to send a stream of data to multiple endpoints in one single pass—you could deploy this fat image to as many PCs as your staging infrastructure could support. In this way, one technician could easily deploy up to fifty PCs in one half day. And, since the PC contained all of the generic content your users required, many of these PCs—sometimes more than 50 percent—were ready to go as soon as the core image was deployed.

Chapter 6 introduced the concept of a ‘thin’ image. This concept was introduced in conjunction with the use of application virtualization for software management and distribution. This meant deploying a smaller OS system image, and then, deploying a generalized application layer (GAL) to achieve the same result you would obtain with a fat image (see Figure 7.4).

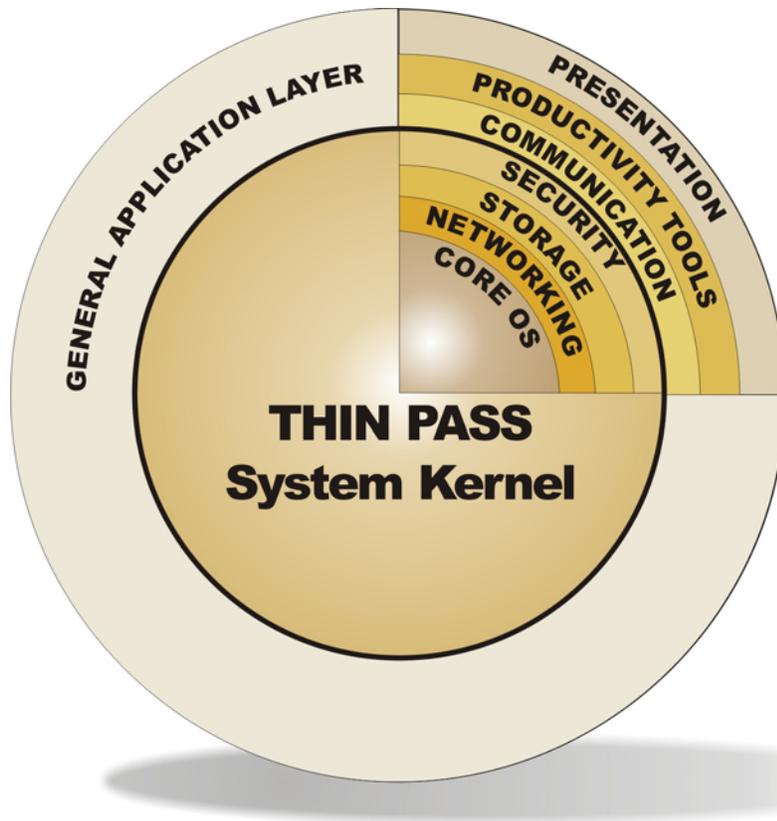


Figure 7.4. The Thin Kernel with the GAL

Consider the following points as you determine whether you should use a fat or a thin image:

- If you use a fat image, you can use multicasting technologies to deploy it in a single pass to multiple endpoints.
- If, however, you use a fat image, then, maintaining and patching the content of this image can be challenging because it contains so many different components that all have their own update cycles.
- If you use a thin image and you are relying on traditional application installations, for example, through the Windows Installer service, then deploying the GAL will take time. Office itself is usually in the order of 300 to 400 MB and the entire layer can easily be well over ½ GB. Since multicasting is no longer available for this deployment—at least not through traditional software deployment tools—you then need to perform unicast or point to point deployments to each endpoint, adding considerable time to the installation. This will impact a technician’s ability to deploy 50 PCs per half day.

- If you use a thin image and you are relying on application virtualization with streaming, then you only need deploy the thin kernel to a PC, deliver the PC to the end user (if you are using a staging area), and then have applications from the GAL stream to the PC as soon as the user logs on for the first time. Since applications are streamed, they do not negatively impact network bandwidth. Since applications are controlled through security groups in AD, the process can be transparent and initiated only at first logon. You can also ensure that users are aware of this process through the training program you provide.
- If you are using a thin image—whether you are using traditional or virtualized applications—it will be a lot easier to maintain the system image in the long term because it will include less content. Then the contents of the GAL can be maintained either individually or as a group, but since the GAL is made up of individual packages, each can be maintained on its own.

In the end, it makes sense to work with a thin image as much as possible. In the long term, the thin image will be much easier to maintain and support. It is however, highly recommended that you supplement this management strategy with application virtualization and streaming to reduce application and PC management costs.

### Using a Single Worldwide Image

Traditionally, system images were limited to one specific system type because of the integration of the hardware abstraction layer (HAL) within the image. This meant that organizations needed to create multiple images—in the case of some of our customers, up to 80 images—depending on the size of their network and the number of different PC configurations they had to deal with. But, with Windows Vista, system images are now HAL-independent since the HAL can be injected during the configuration of the image on a PC. Coupled with other Vista features, this HAL independence has several implications in terms of image creation:

- One single image per processor architecture—32- or 64-bit—can now be created.
- The reference computer—the computer you use as the source of the image—can now be a virtual machine since the HAL is no longer a key factor in image creation and deployment. This reduces the cost of maintaining the reference computer and this also makes it easier to keep it in a pristine state.
- Custom hardware drivers can be injected into system images so that your image can be compatible with all PC types in your organization.
- Vista is now language agnostic. The core OS does not have a language installed. The language pack for the installation is selected during the installation process. This means that one single image can now be matched to any of the languages Vista supports.

Creating one single worldwide image per processor architecture is now entirely possible whether you use the WIM image format or not.

## Discovering the Installation Process

 This is the core function of Unit Testing for the members of this PC team.

As you prepare your logical system design and get it approved, you can begin the discovery process for the Vista installation. These pre-imaging processes are necessary as you need to fully understand how Vista's installation works to be able to learn how it will be automated in later project phases. These pre-imaging processes include:

- Identifying the hardware requirements for Vista's installation
- Identifying the installation methods Vista supports
- Documenting the installation process you select
- Using an installation preparation checklist
- Performing post-installation configurations

Then, when you've fully understood how Vista's installation proceeds and what you need to do to prepare your physical OS kernel, you can proceed to the creation of a reference computer and the generation of the system image.

### Identifying Hardware Requirements

Before you begin testing installation methods, you need to determine which hardware configurations you will support. This is derived from a series of information sources including both your network inventories and Microsoft's recommended minimum hardware requirements for Vista. Base hardware requirements for Vista were introduced in Chapter 1 and are reproduced here as a refresher (see Table 7.1). Two sets of requirements are defined: Vista Capable and Vista Premium PCs. The first allows you to run the base-level Vista editions, and the second lets you take advantage of all of Vista's features. Since you're preparing a deployment for long-term management, you should really opt for Vista Premium PCs.

Vista Mode	Component	Requirement
Vista Capable PC	Processor	At least 800 MHz
	Minimum Memory	512 MB
	Graphics Processor	Must be DirectX 9 capable
Vista Premium PC	Processor	32-bit: 1 GHz x86 64-bit: 1 GHz x64
	Memory	1 GB
	Graphics Processor	Support for DirectX 9 with a WDDM driver, 128 MB of graphics memory, Pixel Shader 2.0 and 32 bits per pixel
	Drives	DVD-ROM drive
	Accessories	Audit Output
	Connectivity	Internet access

\* If the graphics processing unit (GPU) shares system memory, then no additional memory is required. If it uses dedicated memory, at least 128 MB is required.

**Table 7.1 Vista system requirements.**

 Information on compatible systems can be found at <http://winqual.microsoft.com/hcl/>.

Next, you need to identify which editions of Vista you will support. For business, the Business, Enterprise, and Ultimate editions are available. Each of these business editions requires a Vista Premium PC to run and includes:

- **Vista Business Edition:** This is the base edition for small to medium business. It includes the Aero 3D interface, tablet support, collaboration tools, advanced full disk backup, networking and remote desktop features.
- **Vista Enterprise Edition:** This edition is only available to organizations that have either software assurance or enterprise agreements with Microsoft. It adds full drive encryption, Virtual PC Express, the subsystem for UNIX and full multilingual support.
- **Vista Ultimate Edition:** This edition is for small businesses or others that want to access the full gamut of new Vista features but do not necessarily want software assurance or an enterprise agreement. It includes all of the features in the Enterprise Edition, but also entertainment tools such as Photo Gallery, Movie Maker and Media Center. Though you might not want these programs on business computers, this edition might be the only choice for any organization that wants full system protection and does not want to enter into a long-term software agreement with Microsoft.

Remember that through its single instance store capability, a Vista image may contain more than one edition. If you need to rely on several editions, you can still store them into one single image.

 To learn more about each of the different Vista Editions, go to <http://www.microsoft.com/windows/products/windowsvista/editions/default.aspx>.

Also, since you will be relying on virtualization software to create and manage the reference PC, you should configure this VM according to the capabilities outlined in Chapter 3. In fact, the virtual machines for Unit testing should already be available to your team.

### ***Identifying Installation Methods***

Now that you have identified your logical system configuration and you have selected the base PC configuration, you can proceed to the examination of Vista's installation methods. The first and the easiest method to examine is the interactive installation. No matter what you choose to do in the end to automate your installation, you will definitely need to perform at least one and most probably several interactive installations so that you can fully understand what happens during this process.

The objective of this process is the documentation of each step of the installation and specifically, the build of your entire kernel.

- Begin by choosing the edition of Windows Vista to install.
- Perform the initial installation to discover the process.
- Document every configuration requirement and each modification you need to perform.
- Document the finalization steps to create your thin system kernel.
- Document each step to create and configure the GAL.

First, you need to understand how the basic interactive installation works. With Windows Vista, Microsoft simplified the installation process to ensure there were no more blockers for the installation to complete. In previous versions of Windows, there were several instances during the installation where you had to provide input: CD keys, time zone, keyboard layout, regional settings, administrative password, networking configuration, and more. Now, Microsoft has modified the installation to collect all information at the very beginning of the process and then have you finalize the configuration once setup is complete. This means you can start multiple interactive installations and do something else while they run, returning to them once they have completed. And, since machines are setup in a locked down state, you don't even need to worry about the setups being vulnerable when you're not there.

Unlike previous versions, the Vista installation is completely graphical. The installation now boots into the Windows Preinstallation Environment (Windows PE) if there is no operating system on the PC. And if there is a previous operating system and the upgrade is supported, the installation will run in graphical mode anyway. The first splash screen will ask three questions:

- Language to install
- Time and currency format
- Keyboard or input method

These settings determine in which language the installation will proceed as well as which language pack will be installed. Vista uses a language-agnostic core installation that is then converted into whichever language you select during installation.

Next, you are presented with the **Install now** screen. Note that this screen also includes two additional options in the lower left corner:

- What to know before installing Windows
- Repair your computer

The first provides you with up to date information on system requirements and procedures for installing Vista. It is always a good idea to review this information, especially during the installation discovery process. The second is used to repair systems that may be damaged. It lets you choose an existing system partition, and then when you click **Next**, you are presented with a series of choices for system repair (see Figure 7.6) including:

- Startup Repair: to fix problems related to the startup of Windows.
- System Restore: to restore Windows to an earlier point in time.
- Windows Complete PC Restore: to restore Windows from a backup image.
- Windows Memory Diagnostic Tool: to verify the system's memory.
- Command Prompt: to launch a Windows PE session with an open command prompt.

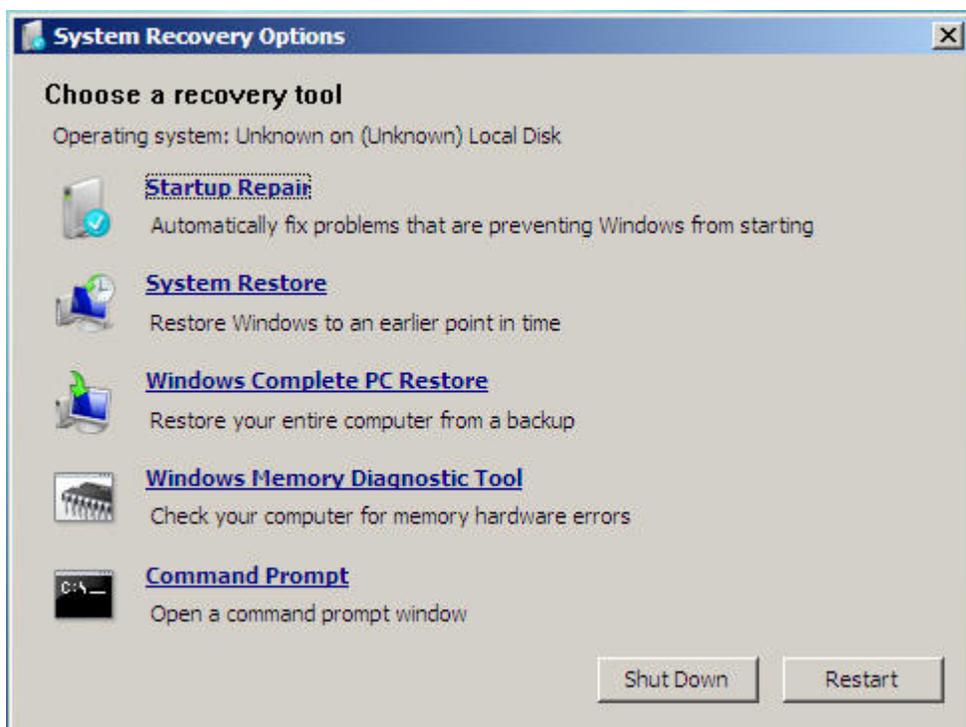


Figure 7.5. System Repair Options

But, since your goal is to discover how the installation works, click on **Install now**. This moves you to the next screen where you need to input the product key to use for the installation. The version you install will be determined by the product key you enter. Note that this screen also includes an automatic activation check box. If you are only exploring the installation and may repeat it several times, you will probably not want to turn this option on.

The next screen is where you accept the license agreement, click **Next** and you are then moved to the installation type selection screen. Two main options are available:

- **Upgrade:** select this option if there is already a supported operating system on your PC.
- **Custom (advanced):** select this option if you are installing a new PC or if the PC you are upgrading is not running a supported operating system for upgrade.

 The upgrade process in Vista actually works! That's because every installation of Vista uses an image to perform the installation. Remember IBS? Because of IBS, the upgrade actually removes all previous operating system components, protects all data and application settings as well as all installed applications, and then installs Vista by decompressing the installation image and customizing it to the hardware you are installing it to. You should investigate this process if you are running supported systems for upgrade.

If you are installing on a bare metal system or a bare metal virtual machine, then select the second option. This will lead you to a screen where you can select and create the disk partition that will run the OS. This screen also gives you access to partitioning and formatting tools as well as giving you the ability to load new drivers. Examine each option and then proceed with the installation.

 **BitLocker Partitions:** If you intend to run BitLocker and encrypt the system partition, then you need to create two partitions. The first should be at least 2 GB in size, should be formatted as NTFS and should be marked as active. This will be the boot partition once BitLocker is activated. The second should also be NTFS and should normally use the remaining space on the system disk.

 **WinRE Partitions:** You can also install a Windows recovery environment (WinRE) on the PC. In our opinion, these partitions should be reserved for critical systems and shouldn't be installed on each system because they are used to repair installations (remember that you can get to this with an installation DVD). After all, once you'll be done with your system kernel, you'll be able to deploy it to any PC within half an hour. It usually takes longer than that to repair a PC. But, if you want to use WinRE anyway, consider these options:

- ➔ **WinRE Partitions without BitLocker:** If you intend to install WinRE on the PC, then you'll need the same kind of partition as you would for a BitLocker system.
- ➔ **WinRE Partitions with BitLocker:** If you install both BitLocker and WinRE, then you need to install WinRE into the OS partition to protect the system from tampering through WinRE. Do this once the OS and BitLocker are installed.

Once the partition is created or selected, Windows begins the installation process. From this point on, there is nothing to do until the installation is complete. The installation will copy the Windows installation files, expand them, install features, install updates and then complete the installation. During this process, Windows will install and reboot into an open session once the installation is finished.

### Installing x64 Operating Systems

- ➔ If you're installing an x64 version of Vista, you will run through the same process as for x86 versions with minor differences. For example, the x64 OS will support a non-destructive upgrade from x86 OSes—that is, replacing the existing OS and maintaining data on the system—but the end result will retain all data as well as application folders except that applications will be non-functional and will need to be reinstalled. The best way to perform this type of installation is to actually move the data off the system if there is data to protect, then reformat the OS partition and install a fresh version of the x64 OS.

The installation process includes five (5) steps. The system will restart several times during the installation:

- Copy Windows files
- Expand files
- Install features
- Install updates
- Complete the installation

There is no time-to-finish information display anymore; instead it displays the percentage of each step. It can take between 20 to 40 minutes for an installation to complete, depending on system configurations.

Once the installation is complete, Vista displays a **Set Up Windows** dialog box requiring a user name and password. Remember that Vista automatically disables the default administrator account. Therefore a core account is required. Though this account will be a member of the local administrators' group, it has a different security identifier (SID) than the default administrator's account and will therefore be subject to User Account Control (UAC).

Type the username, then the password, confirm the password and type a password hint if you need it. Click **Next** when ready. The next screen requests a computer name and description. Type these values in and click **Next**. The third setup screen lets you set up the update configuration. Choose the configuration that suits your environment. Now, you need to indicate the time zone, time and date. Click **Next** when ready.

The last screen lets you identify which network you are connected to. Each choice sets different parameters in the Windows Firewall. Choose **Work** and then click **Start** on the Thank You! Screen. Vista completes its configuration, checks your computer's performance, and displays the log on prompt.

When you log on, Vista displays the **Welcome Center** (see Figure 7.6). This center displays a summary of the results of your installation. The first part displays a summary of the computer's configuration. The second lists tasks to complete in order to finish the installation. And the third displays offers from Microsoft. For example, this is where you would download and install Windows Live Messenger.

The most important part of this screen is the second part because it deals with activities required to complete the system's configuration. Usually thirteen items are listed in this section, but of course, since this is a summary, not all items are displayed. To display all items, you need to click on **Show all 13 items**. This expands the section and lets you see each item in the list.

This Welcome Center is oriented mostly towards the home user, but it can be useful for newcomers to Vista installations and configurations to peruse through the choices it offers in order to become more familiar with Vista itself.

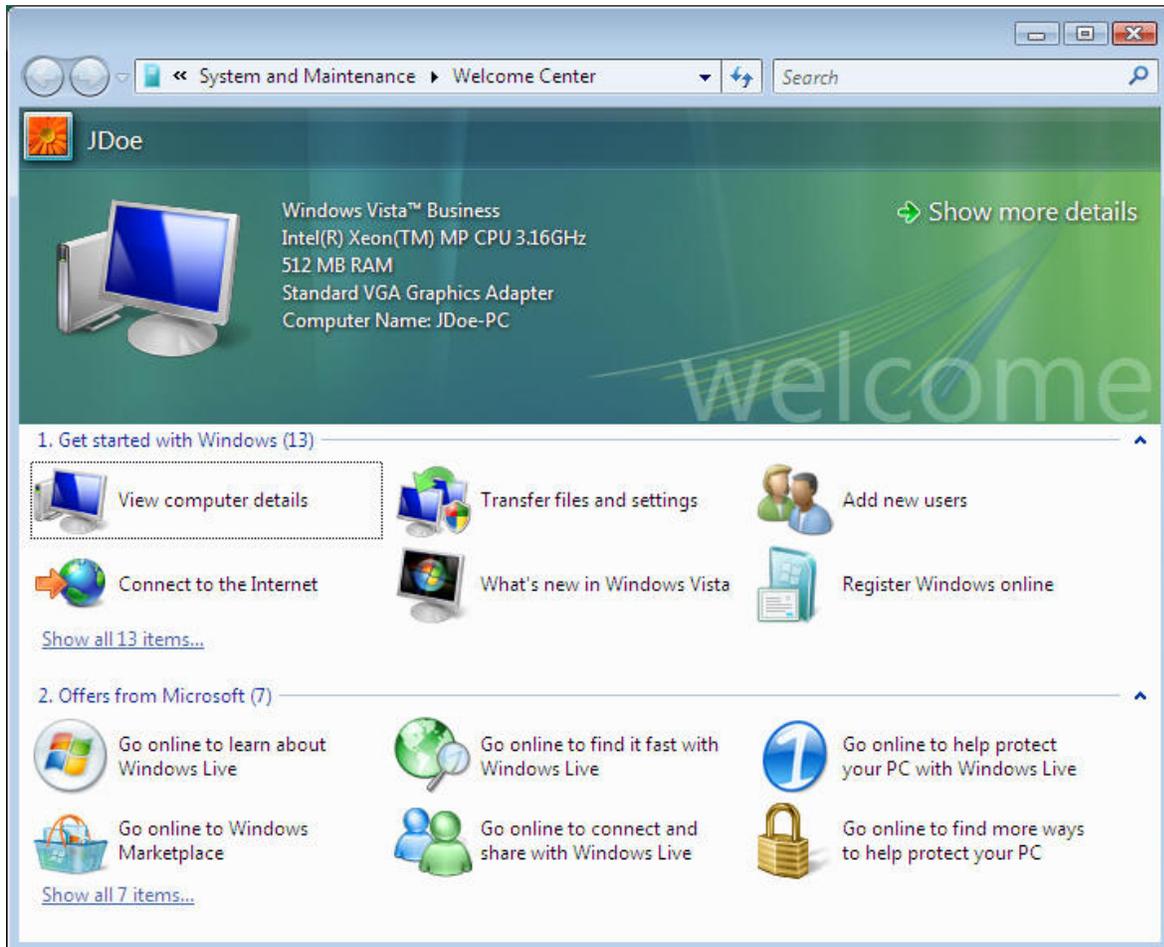


Figure 7.6. The Vista Welcome Center

### Using Installation Documentation

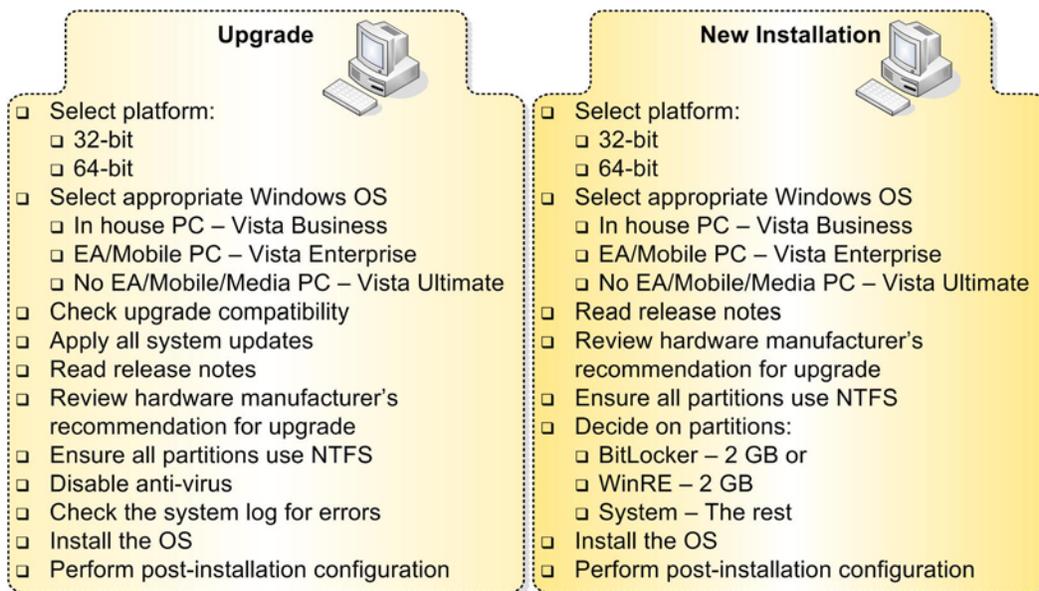
Now that you are familiar with the installation process, you can begin the configuration process for the remainder of the kernel layers. This is an ideal time to implement installation documentation and begin your installation documentation process. Focus on three activities:

- Installation Preparation
- OS Installation
- Post-Installation Configuration

Each requires specific documentation.

## The Installation Preparation Checklist

In this type of migration project, you want to make sure that everyone performs the same operations all the time. The best way to do this is to prepare specific checklists for operators to follow. For example, you should use a recommended checklist for installation preparation (see Figure 7.7). It is possible to upgrade from Windows 2000 or XP to Vista. This checklist takes this consideration into account.



**Figure 7.7: The Installation Preparation Checklist**

The installation checklist takes a few items into account:

- In the Upgrade, remember that there is no upgrade path from 32-bit to 64-bit.
- Vista Editions are selected based on whether the PC will remain in the office (in house). If this is the case, you can use Vista Business because it does not include BitLocker.
- If the PC is mobile, then you may need a Vista edition that includes BitLocker. If you have volume licensing or an enterprise agreement (EA), then you can use Vista Enterprise. If not, then you must use Vista Ultimate.
- If you upgrade and retain the existing partition, you cannot install BitLocker as it requires an extra partition.
- If you are performing a new installation, then you can partition the system for either BitLocker or WinRE.

These considerations will help you prepare for your own installations.



This checklist is not a checklist for PC replacement or deployment. It is intended only for PC technicians working to discover the installation process.

## Documenting PC Installations

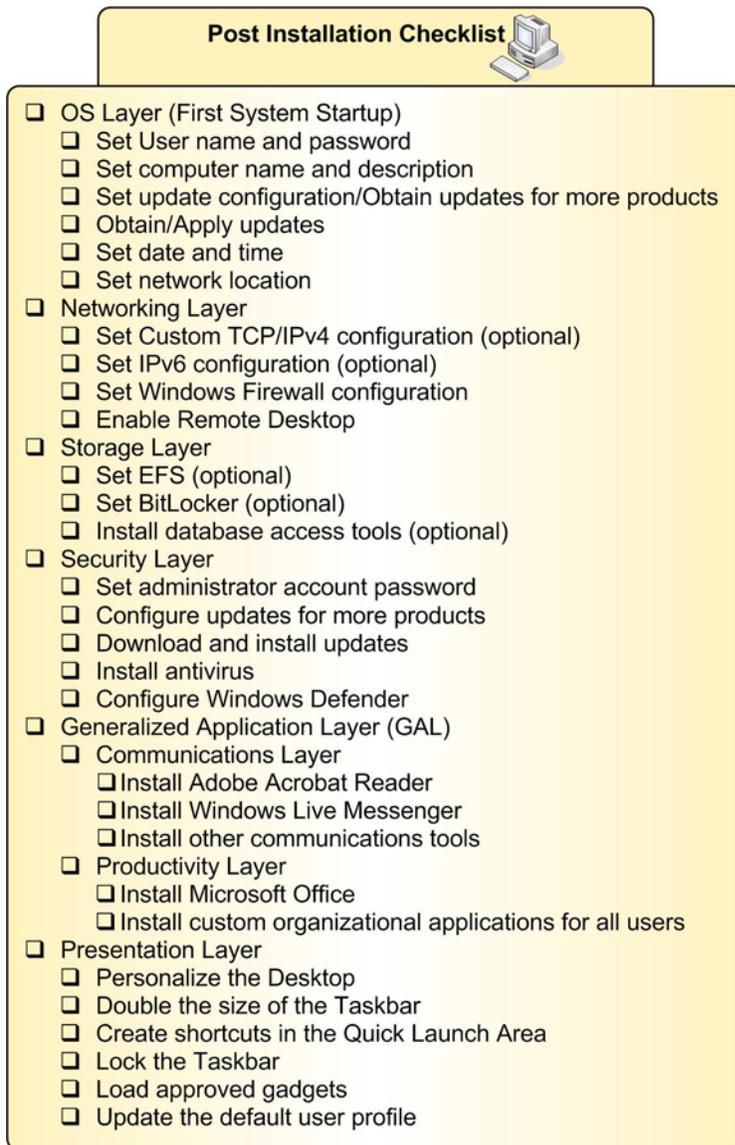
In addition, you'll need to document the PC installation itself. The best way to do this is to use a standard PC Data Sheet. This sheet should include vital information such as:

- System Name
- System Role
- System Location
- Hardware Specifications
- BIOS Version
- Disk Partition(s)
- Kernel Version (including Operating System Versions, Service Packs and Hot Fixes)
- Installed components
- Any additional comments or information you feel is required

Ideally, this data sheet will be in electronic format so that data can be captured as the installation proceeds. It can also be adapted to database format. In support of the PC installation, you might also create a Kernel Data Sheet outlining the contents of the PC kernel for this particular version of the kernel. Each sheet should provide detailed and up to date information to technicians.

## Post-Installation Processes

After the installation is complete, you'll want to perform a post-installation customization and verification (see Figure 7.8). Use a post-installation checklist to customize the system and to perform a quality assurance verification of the installation. This checklist also lets you complete the installation and preparation for the system kernel.



**Figure 7.8: The Post-Installation Checklist**

The activities outlined in this checklist are detailed further in this chapter.

## Supported Installation Methods

Windows Vista offers four installation methods:

- Interactive
- Unattended with an Answer File
- System Imaging with the System Preparation Tool
- Remote OS Installation through Windows Deployment Services

You may end up using each of these as you proceed through the preparation of your installation process. For example, you need to use the interactive installation to perform the discovery process. Then, the unattended installation will be required in two instances: the upgrade, if you choose to use it, and the build of the reference computer. You'll use system imaging for both computer replacements and for bare metal—computers with no OS installed—installations. And, if you need to support remote deployment of the OS, you may use Windows Deployment Services. In fact, this is one of the decision points that must arise from this discovery process: choosing which installation methods you will decide to support (see Figure 7.9).

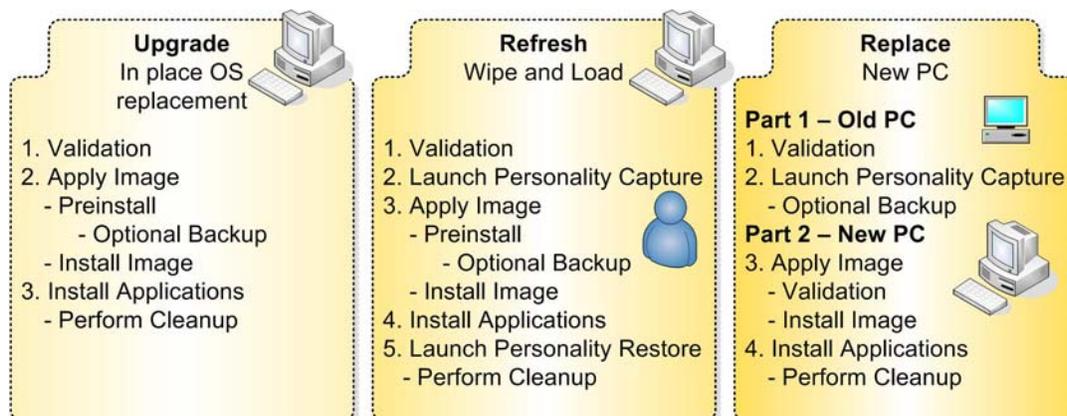


Figure 7.9. Selecting an Installation Method

## Selecting an Installation Process

Based on these different options, you can select which installation scenarios you will support:

- **Upgrade** which aims to replace the existing operating system without damaging data or installed applications.
- **Refresh** which is a wipe and load approach where the system disk is wiped out, reformatted and a new operating system is installed.
- **Replace** where a brand new or bare metal system with no existing operating system is prepared and a new OS is installed.

Each scenario focuses on a specific massive installation method. Few people have supported or opted for the upgrade path in the past. This may once again be the case because of the limitations of the upgrade path. For example, if you want to enable BitLocker drive encryption, then you cannot use the upgrade because you need to repartition the disk drive. Of course, you could use a disk partitioning tool, but it is easier to just perform a new installation. Another instance where the upgrade does not work is upgrading from a 32-bit OS to a 64-bit OS. In the end, you will decide if the upgrade process is useful for your organization. If not, then you will focus on the other two scenarios. In every case, you need to create a physical OS configuration before you proceed.

## Determining the Physical OS Configuration

 At this stage, you should be moving into the Functional testing level.

Now that you've discovered the installation process and you have documented the steps you need to perform it, you can move to the creation of your physical OS configuration. This focuses on the creation of the reference computer. Keep in mind that when you do this, you need to make sure undoable disks are enabled in the virtual machine (VM) you will be using. This way, you can be sure to capture only settings that you are absolutely happy with. If you make a mistake, reset the VM and start the step over. This activity focuses on the post installation configuration tasks.

You'll also need to use other tools to finalize the preparation process for the reference PC. Be sure to document all configuration modifications you retain. This will be important for when you need to reproduce the reference PC later on. Your documentation must also be specific; i.e., you must specifically detail the steps you need to perform to complete the core system's configuration.

## Applying the Post-Installation Checklist

This process should include all the steps in the Post-Installation Checklist, but special attention should be paid to the following:

- Setting a strong password for the default administrator account
- Configuring networking
- Enable updates
- Download and install updates
- Enabling the Remote Desktop
- Configuring the Windows Firewall
- Configuring the Windows Vista Interface
- Updating Default User Settings

Perform the tasks as they appear in the Post-Installation Checklist.

Begin with the default administrator account password. Launch the Computer Management console using Run as Administrator. To do so, type **Computer Management** in the **Search** bar of the **Start Menu**, then right-click on **Computer Management** to select **Run as Administrator**. Approve the UAC prompt. Then, move to **Local Users and Groups**, then **Users** and right-click on the **Administrator** account in the details pane and choose **Set Password**. Assign a complex password. This password should include at least eight (8) characters and include complex characters such as numbers, uppercase and lowercase letters, as well as special characters.

If you have difficulty remembering passwords, you can replace letters with special characters. For example, replace the “a” with “@”, replace the “o” with “α” and so on. This makes passwords more difficult to crack. Even so, if a hacker or an attacker has access to the system, they can use password cracking tools to display the text of the password. If this is an issue, you can use a combination of Alt plus a four digit Unicode key code to enter characters into your password (for example, Alt 0149). The advantage of this method is that these characters often display as a blank square or rectangle (□) when displayed as text by password cracking software. If you’re really concerned about password security, then either use more than 14 characters—password-cracking tools stop at 14—or implement a two factor authentication system for IT administrators.

It might also be an idea to rename this account. Make sure you keep it disabled.



The default administrator account in Windows Vista is a special account that is not subject to User Account Control. Other accounts that are members of the local administrative group are, on the other hand, subject to UAC. If you develop a policy around UAC use on your network, leaving the default administrator account disabled will ensure that every user—administrative or standard—will be subject to the rules of your UAC policy. In addition, you want to avoid the use of generic accounts such as this one because even though its activity is tracked as will all other accounts, you cannot ‘know’ who is using it since it is not a named account. Every administrator and technician in your network should use named accounts for high privileged operations.

Next, use the **Control Panel** to access the **Network and Sharing Center**. Click on **View status** and then **Properties** for the connection you want to configure. By default, Vista installs and enables two versions of the TCP/IP protocol: IPv4 and IPv6. IPv4 is set to receive an automatic address from a server running the Dynamic Host Configuration Protocol (DHCP). IPv6 is set to a private address by default. If you decide to use IPv6 in your network, you'll need to change this address.

The Network Properties dialog box is the same as in Windows Server 2003 so it should be familiar to most administrators. Use your corporate guidelines to assign settings to both IPv4 and IPv6. Close the Network Connections window when done.

 If you plan to use IPv6, and you should because Vista networks can rely on this new communications protocol, you will need to obtain an IPv6 address scope either from your Internet provider or for your own use. IPv6 is enabled and configured by default in all installations of Windows Vista. But this configuration uses a link-local address with the default fe80::/64 address prefix. Link-local addresses are only used to reach neighboring nodes and are not registered in DNS. More useful IPv6 connectivity must be configured either manually or through DHCPv6 which won't be available until Windows Longhorn Server ships later this year. IPv6 scope addresses can be obtained from Regional Internet Registries (RIR). The most common five RIRs are:

- ➔ — American Registry for Internet Numbers (ARIN) for North America ([www.arin.net](http://www.arin.net))
- ➔ — RIPE Network Coordination Centre (RIPE NCC) for Europe, the Middle East and Central Asia ([www.ripe.net](http://www.ripe.net))
- ➔ — Asia-Pacific Network Information Centre (APNIC) for Asia and the Pacific region ([www.apnic.net](http://www.apnic.net))
- ➔ — Latin American and Caribbean Internet Address Registry (LACNIC) for Latin America and the Caribbean region ([www.lacnic.net](http://www.lacnic.net))
- ➔ — African Network Information Centre (AfriNIC) for Africa ([www.afrinic.net](http://www.afrinic.net))
- ➔ Once you obtain your scope, you can use it to configure your servers. Configuration of IPv6 settings is very similar to that of IPv4. You need to configure the following settings:
- ➔ — IPv6 unicast address
- ➔ — Subnet prefix length—by default this is 64
- ➔ — Default gateway—again in IPv6 unicast format
- ➔ — Preferred & alternate DNS servers —again a unicast address
- ➔ You can use the advanced settings to add either multiple IPv6 addresses or additional DNS servers. There are no WINS servers for IPv6 since it does not use NetBIOS names.

You should also enable updates according to the settings in your organization. Select **Control Panel, Security, Windows Update, Change Settings** to modify the update settings. Make sure you have enabled updates for more products and then set the update value according to your organizational standards. It is a good time to apply all available updates to this system.

 **Reference Computer:** The networking properties for the reference computer might best be left at default values unless you have specific values you can use for default settings. Remember that whatever is configured in the reference computer will be retained in the system image you create from it.

Use **Control Panel, System and Maintenance, System, Remote Settings** to enable the **Remote Desktop** option. Click on the **Remote** tab and select the appropriate setting. The most secure setting uses Network Level Authentication, but requires connections from systems running the Remote Desktop Connections 6.0 client update. Make sure this update has been deployed in your network before you deploy Vista systems. You also note that Remote Assistance is on by default.

Use **Control Panel, Security, Windows Firewall** to set the default Firewall behavior. The Firewall is an element of Windows that can be controlled through Group Policy. Make sure this configuration is in the base configurations for all Vista systems.

Now configure the Vista interface. Turn on the **Windows Sidebar** and apply the gadgets you need. Then, customize the **Quick Launch Area**. You want to do this to ensure that every user in your organization will have the same or at least a very similar experience whenever they access a PC. Begin by doubling the size of the **Taskbar**. Do so by moving the mouse pointer to the top of the Taskbar beside the Windows Start button until the pointer transforms into an up-down arrow. Click and drag upwards to expand the Taskbar.



#### Using internal Really Simple Syndication (RSS) feeds

- ➔ You can rely on the RSS feeds gadget to send internal communications messages to end users through the Vista Sidebar. This way, organizations can send internal messages to all users. All you need is a Web page that provides RSS feed information, a subscription to this feed in the Vista PC and the appropriate feed displayed in the gadget. One gadget can be used to connect to each feed you want to use. Departments, the organization as a whole and IT can all use these feeds to display key information to the user base without clogging the desktop. This is a simple and easy way to communicate with users without having to implement complex communications systems.

The Taskbar includes running programs as well as the Quick Launch Area. Each area is preceded by a row of four series of dots at the very left of it. Move the pointer on top of this row for the running programs list until it turns into a left-right arrow. Click and drag the running programs bar to the bottom left of the Start button. Now you should have running programs displayed below the Quick Launch Area. Right-click on the taskbar and select **Lock the Taskbar**.

Next, click on the **Start** button, then on **All Programs** and run through the default programs to add the ones users will use the most to the Quick Launch Area. To add each program shortcut, right-click on it and select **Add to Quick Launch**.

Add the following items:

- Under Accessories:
  - Calculator
  - Command Prompt
  - Notepad
  - Windows Explorer
- Under Accessories | System Tools:
  - Character Map
  - System Information

The resulting Taskbar should include most of the tools anyone will need to use to interact with PCs in your organization. The Quick Launch Area should be updated each time a new common tool is added to the system. Order the tools in the order of most used from left to right (see Figure 7.10). Your interface is set.



Figure 7.10: A well-managed PC Taskbar

### **Update the Default User Profile**

Whenever a new user logs on to a system for the first time, Windows generates a new profile for them by copying the contents of the default user profile. If you customize your environment and then update the default user profile from your customized environment, you can ensure that each time a new profile is generated it includes a core set of tools and interface enhancements. In an organization that wants to ensure that all of their users rely on a standard computing environment, updating the default user profile is absolutely essential.

Return to the Computer Management console to create a second administrator account. This account may or may not be required according to your organization's security policy, but it is required at least temporarily to update the default user profile. Expand **Local Users and Groups**, then right-click on **Users** to select **New User**. Name the account **BUAdmin**—or use your organizational standard—give it a full name of **Backup Administrator**, add a description, give it a strong password and assign the **Password never expires** right. Click **Create**, then **Close**. Next, right-click on **BUAdmin** and select **Properties**. Move to the **Member Of** tab, select **Add**, once the dialog box opens, click **Advanced**, then **Find Now**, double-click **Administrators** and **OK**. Click **OK** to close the dialog box. Your account is ready.

Vista does not allow you to copy an open user profile to another because many of the open features are volatile and are therefore stored in RAM and not persisted until the user logs off. So to update your default user, you must use the backup administrative account created earlier. Use the following procedure

1. Log out.
2. Log into your **backup administrator** account. Vista creates a new profile based on old settings.
3. Open **Windows Explorer** and set **Folder Options** to view hidden files.
4. Use **Control Panel, System and Maintenance, System, Advanced system settings** and the **Advanced** tab to click on the **Settings** button under **User Profiles**. Select the profile you customized and click the **Copy to** button.
5. Use the **Browse** button to navigate to the **Users** folder on the C: drive to find the **Default** profile. Click **OK**.
6. Click **Yes** to replace existing files.
7. Close all dialog boxes and log off of the **backup administrator** account.
8. Log back into **your original account**.
9. Launch the **Control Panel** and select **System and Maintenance, System, Advanced System Settings** and click on the **Settings** button under **User Profiles**.
10. Select the **backup administrator's** profile and **delete** it. Confirm deletion.
11. Close all dialog boxes and go to the Start button and use the right arrow beside the lock to select **Switch Users**.
12. Log into the **backup administrator's** account. This will test the default user profile. Note that you now have a copy of the customized profile. Log off BUAdmin.

You're done. You still need to complete the discovery process, especially with reference to the GAL components. Remember, each time you add a new component to the system kernel, you should make sure the Quick Launch Area and the default user profile are both updated.

Keep the reference PC in a workgroup. This will make it easier to manage. Also, keep the BUAdmin account on the reference computer so that you can use it in the future to update the default user profile. Remember to remove it from the copy of the reference PC you will use to create your system image

 If you use application virtualization for the components of the GAL, you can make sure the proper shortcuts appear in the Quick Launch Area by including them in the application capture you perform. This way, they will automatically update the user's profile when the virtualized application is streamed to their system.

You should repeat the process to create a new reference computer. If you've documented each of these steps, you should be able to repeat this process without flaw. This reference computer will be the model you use for your massive installation method.

 Windows Activation: Do not activate the installation as you are performing discovery. You have thirty (30) days to do so which is ample time to perform the discovery. You can, however, activate the reference computer since it will be a machine you keep on a permanent basis.

## Determining the OS Deployment Method

 This activity is part of the Organize phase of the QUOTE system.

Now that you fully understand how the interactive installation process occurs and you know how to build your reference PC, you can proceed to the next step: determining how you will be performing massive deployments of this OS. As mentioned earlier, there are several tools and processes you can use. Microsoft has delivered a series of tools in support of the image-based setup Vista supports. Other vendors have updated theirs to work with Vista. Both Microsoft and third parties tools support one interactive and three automated deployment strategies.

- The first is the interactive installation. In organizations of all sizes, this installation process is really only used for discovery purposes. After all, no one wants to have their technicians go from PC to PC installing Vista interactively. Even with a very well designed instruction sheet, this method would definitely give you mitigated results. Only very small shops would use this method. But even then, they will not have a method for system rebuilds since everything is manual and interactive. In the long run, it is always best to use an automated method.
- The second is the unattended installation based on a response file. With Vista, Microsoft has reduced the number of response files to one; well two really, but they are the same file. Response files are now in XML format and are named Unattend.XML. Using a response file automatically feeds input to Vista during its installation, letting you go on with other tasks as the system installs itself. The second response file is the AutoUnattend.XML. This file uses the same content as the original file, but its name allows it to be automatically applied when it is provided either through a USB memory stick or through a floppy drive during installation. Just insert the Vista DVD, insert the memory stick or the floppy and boot the machine.

- Unattended installations are usually valid for organizations with very few computers.
- Larger organizations will rely on this unattended installation method to reproduce their reference computer when they need to rebuild it.
- Unattended installations are also useful for in-place upgrades. Even today, few organizations choose to perform these and take advantage of OS migrations to ‘clean’ house and reset each and every one of their PCs.
- The third method is the system image. This system image relies on the capture of a copy of an installed system. This copy is depersonalized first through the use of a special command: Sysprep.exe. This tool is now part and parcel of every Vista system. Sysprep is located in the %SYSTEMROOT%\SYSTEM32\SYSPREP folder. This tool is designed to prepare a configured system for redistribution. Then, you capture the system image with another tool to reproduce it on other computers.
- The fourth method is the remote OS installation. With Microsoft, this means using Windows Deployment Services (WDS), an update which is available for Windows Server 2003 through Service Pack 2. WDS replaces the previous remote installation services delivered with Windows 2000 and supports the remote deployment of Windows XP, Windows Server 2003 and Windows Vista. WDS requires a complex support architecture including Active Directory, DHCP, and DNS to operate. Special procedures must be used to put it in place. If you already use or have selected third party OS deployment tools, you will not use WDS, but rather rely on these more comprehensive tools for this type of deployment. But one thing is sure, the remote OS deployment method is by far the most popular since it relies on the creation of a system image first, and then, provides you with a tool to remotely deliver this image to any PC endpoint whether you rely on WDS or a true systems management tool.

The selection of the appropriate deployment method is a key activity for the PC team responsible for system imaging.

Microsoft has also released other tools that will make the preparation of your system images easier to work with. They include:

- The **Windows System Image Manager** (Windows SIM) which is used to build and customize automated installation answer files.
- **WinPE** which is a 32-bit operating system that has only a 24-hour duration at any given time—it can only run for a maximum of 24 hours at a time, though it can be rebooted any number of times—and includes a limited set of services. WinPE is aimed at preinstallation and deployment of Windows Vista.
- **ImageX** which is a command-line tool that supports the creation and manipulation of system images for installation and deployment. ImageX is limited in that it is command-line only and does not support image multicasting. Deployments using ImageX have to rely on unicast image transfers which can have a negative impact on bandwidth utilization. If you already have or have selected a third party tool for OS deployment such as Ghost Solution Suite or Altiris Deployment Solution, it will have its own system image creation tool and you will not use ImageX.

These tools are contained in the Windows Automated Installation Kit (AIK) which can be obtained from the Microsoft download site at [www.microsoft.com/downloads](http://www.microsoft.com/downloads). Make sure you obtain the latest version of this kit before you begin to prepare for installation automation.

 The Windows AIK is also contained within the Microsoft Business Desktop Deployment (BDD) toolkit. This BDD toolkit can be obtained at <http://www.microsoft.com/downloads/details.aspx?FamilyId=13F05BE2-FD0E-4620-8CA6-1AAD6FC54741&displaylang=en>.

### **Preparation and Prerequisites**

In order to build and test OS image deployments, you'll need a series of other items:

- The **reference PC** you've prepared. This should be running inside a virtual machine since you'll only need it to create the automation system image.
- The **Vista installation media** you want to create images for. Remember that installed versions are controlled by product key so one installation DVD should be enough.
- The **Windows AIK** which you should have already downloaded.
- A **management system** where you will be installing the Windows AIK and perhaps your third party OS deployment tool. You'll use this system to create the system image. This should also be a virtual machine or several virtual machines depending on the prerequisites of the tools you are using.
- Your **build environment** should also be able to simulate a deployment situation. This means a small network. This is one reason why this testing will be performed in the Integration and Staging testing levels because they provide you with a network foundation.
- A **shared folder** on a server to store system images.
- Your physical machine will need to include a **DVD writer** and of course, you'll need blank DVDs to store the new image you create.

The Windows AIK is a CD/DVD image. If you are working on a physical machine, transform the image into a CD and then load it into the CD drive. If you are working with a virtual machine, simply link the ISO file to the CD/DVD drive of the machine and launch the VM.

 The Windows AIK is in .IMG format. If you do not have software that understands CD images in this format, rename the file to an .ISO. It is the same format.

Now you can begin the automation of your Vista setups. Use the following order:

1. Build your reference computer.
2. Copy the files that make up the reference PC virtual machine. Use the copy to create the system image. Remember to remove the backup administrator account before you generate the system image.
3. Create one or more system images.

4. Create an automated response file. Include the product key, system name, custom device drivers, the domain join and language packs in the response file.
5. Deploy the images.

There are hundreds of settings and features you can modify during setup through the response file. Ideally, you will keep these to a minimum and capture information from your reference computer as much as possible. This is the benefit of a system image—it includes all of the configuration parameters you set up on the reference PC. The response file should only include items aimed at customizing your standard image and personalize it as you apply it to each PC.

Once your base image is ready, you'll need to roll it out through a management platform. Most business systems shipped over the last 5 years adhere to the Wired for Management (WfM) specification. These machines support powerful management technologies like Wake-On-LAN (WOL) and Preboot Execution Environment (PXE). Together, these technologies offer support for centrally managing the deployment and configuration of networked computers.

Imaging tools that support PXE and WOL can remotely power on machines and rollout images after hours while users are away. Some solutions can actually group disparate tasks together and execute them as single workflow—they can schedule a personality backup, image rollout and personality restoration to occur in a single, sequenced and automated event. Users arrive the following day and resume work as usual with little impact on their productivity.

This is the focus of the image capture and deployment testing process: identifying each and every step that is required to install a system image on a variety of PC configurations and reproducing this process on an ongoing basis. Make sure the tools you use support this approach. You should also rely on multicasting for image deployment. Ideally, the image deployment tool you use will support the use of multicasting proxies. Proxies let you designate a target system in a remote LAN as the source for the multicast broadcast to that LAN. This avoids the need for modifying router and switch configurations so that they can support multicasting over the WAN.

## Build a Smart Solution

System imaging is the key to the entire OS migration project. It is the most important aspect of this project as it outlays the foundation of your future network. Building a system and then capturing it for reproduction must be done carefully and with great precision. This is why the preparation of your logical solution is such an important step in the process. This lets you properly design the systems you will deploy.

Using application virtualization along with a thin PASS system kernel will let you build smart stability within your network. Each PC will have a pristine copy of the system kernel and you will have the ability to maintain this pristine state on each and every system in your network. Your management solution will maintain the OS kernel, patching and updating it as necessary. Your application virtualization and streaming solution will manage the state of each application on the deployed OS. Your technicians will have fewer issues to deal with—if something doesn't work right, just redeploy the system image. Since applications are streamed and only cached locally, they will automatically reinstall themselves. And, with the proper personality protection approach, your users' data will also be protected. It's that simple.

Make sure that you thoroughly test each aspect of your PC image creation and deployment process. Using the highest quality standards will ensure you make this the best deployment ever.

## Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit <http://nexus.realtimepublishers.com>.