

Realtime
publishers

"Leading the Conversation"

The Definitive Guide™ To

Vista Migration

sponsored by



altiris®

*Danielle Ruest
and Nelson Ruest*

Chapter 5: Security and Infrastructure Considerations	108
Perform Initial Inventories	111
The Inventory Assessment Tool	112
Technical Requirements for Inventory Tools	116
Collecting the Basic System Inventory	117
Server-based Operations in the Lab	120
Build the Host Servers	120
Build Central Laboratory Services.....	122
Participate in the Solution Design.....	123
Prepare the Detailed System Inventory.....	123
Validating Inventories.....	124
Rationalize Everything.....	124
Perform the Inventory Handoff.....	126
Perform a Profile Sizing Analysis.....	127
Perform Project Engineering Activities	128
Vista OS Management Infrastructures.....	131
Manage Vista GPOs.....	132
Manage Vista Folder Redirection	136
Manage Vista Security	136
Manage Vista Event Logs.....	137
Manage Vista Licenses	138
Support the Operations Team	139

Copyright Statement

© 2007 Realtimedpublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimedpublishers.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 Realtimedpublishers.com, Inc or its web site sponsors. In no event shall Realtimedpublishers.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.

Realtimedpublishers.com and the Realtimedpublishers 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 Realtimedpublishers.com, please contact us via e-mail at info@realtimedpublishers.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 5: Security and Infrastructure Considerations

This chapter begins the preparation of all of the engineering tasks required to perform the deployment. Once again, it follows the Desktop Deployment Lifecycle (see Figure 5.1) as well as the PC Migration Cycle. The project has now moved from the preparation phases, including Question and Understand and is beginning the Organize phase of the QUOTE System. There is however, one part of the activities listed here that is required as input to both of the first two phases: initial inventories, especially if you don't have existing inventory capabilities.

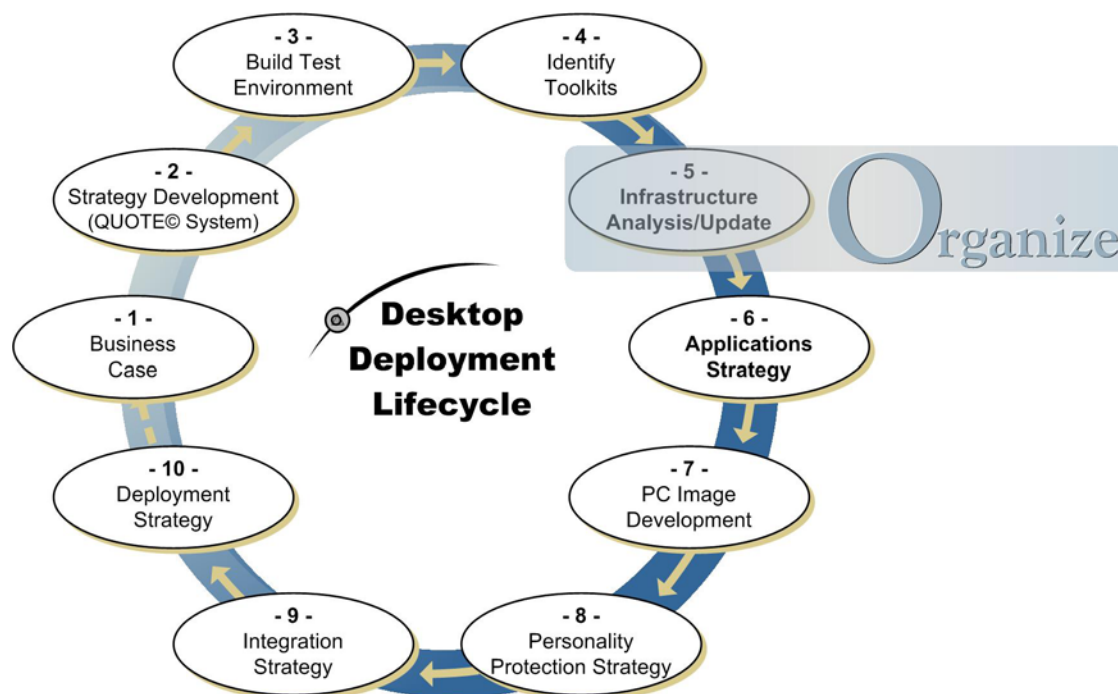


Figure 5.1. Moving through Step 5 of the DDL

The activities of Step 5 of the DDL are performed now because they are required to support the remainder of the engineering process. While most of the other engineering activities will focus on the PC—desktop or laptop—the activities related to infrastructure preparation and security configuration are focused on services provided through the network and therefore affect server structure and may even affect router and switch configuration. In our experience, most organizations do not allow PC support or administration groups to modify the services the network delivers. Because of this, the activities related to Step 5 must involve a server-based group of administrators (see Figure 5.2).

This group should include the following roles:

- A technical architect who will provide direction and evaluate the impact of changes on the network and network services.
- A security expert who may be the same as the one used in the PC team, but who must be focused on server aspects for now.
- A group of technicians focused on:
 - Inventory
 - Application compatibility
 - Deployment
 - System integration
- Support and operations staff to learn new ways of doing things.

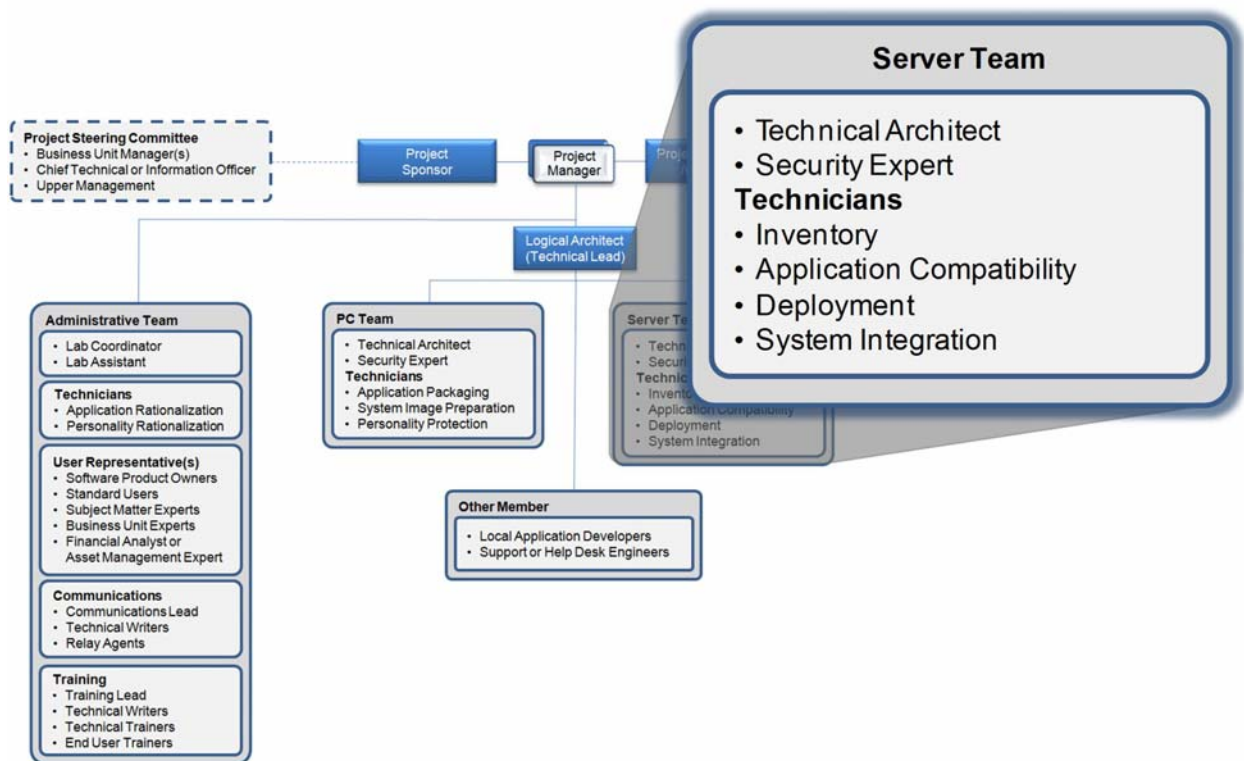


Figure 5.2. The Server Team is responsible for the activities of Step 5

The entire group will be under the supervision of the logical architect or technical lead. In addition, this group must be integrated to the team as a whole as they will need to communicate with their PC counterparts in order to properly discover the expected changes on the network. As such, this group will be responsible for the following activities:

1. Gathering inventories in support of the initial situation analysis
 - Deploying inventory gathering tools if they are not available
 - Performing inventory analysis
2. Support and server-based operation within the testing lab
 - Create central data repositories
 - Build host servers
 - Install virtualization technologies
 - Install collaboration technologies
3. Support for detailed inventories, creating an exact image of what is on each system
4. Support for profile sizing analysis, to help determine required server space
5. Project engineering activities for servers and networks
 - Prepare central and distributed data repositories in support of the deployment
 - Prepare and implement an application compatibility database
 - Install the Microsoft Application Compatibility Toolkit (ACT) version 5.0 if you decide to use it
 - Deploy the ACT client (in conjunction with the PC team)
 - Prepare application packaging systems
 - Prepare data repository shares in support of the PC team, mostly for documentation and user profile captures
 - Configure share replication in multi-site environments
 - Prepare operating system deployment tools
 - If tools exist, then update them to support Windows Vista deployments
 - If tools don't exist, then deploy them in the network
 - Support the various migration scenarios
 - Ensure that network equipment fully supports the deployment technology
6. Prepare Vista OS management infrastructures
 - Prepare for Vista Event Log management
 - Prepare for Vista Group Policy management
 - Active Directory preparation
 - Security considerations
 - Document management considerations
 - Prepare for Vista license management
7. Support the operations team in preparing for the administration of Vista PCs

Generally, the job of the server team is to perform any task that affects servers or network components and provide server-based support to the deployment project team. This assistance occurs both within and without the lab environment.

Inventory and other tools are discussed with a focus on organization size. Three sizes are considered:

- Small organizations (SORG) are organizations that have only one location or site. They usually include less than 100 employees.
- Medium organizations (MORG) are organizations that have at least two locations or sites and thus need to deal with connectivity issues. They usually have up to 1,000 employees.
- Large organizations (LORG) are organizations that have multiple sites, often in different geographical zones that may include multiple languages. These organizations have the most challenging deployments and require extensive planning before the migration can be performed.

Each type of organization has different needs, but mostly in terms of scale, not in terms of actual services required in support of the migration.

Perform Initial Inventories



These activities are part of the **Question** phase of the QUOTE System.

A lot has been discussed about performing inventories in previous chapters, all with the purpose of leading up to this point—the point where you actually perform the inventory. Two inventories are required. The first is the initial inventory which is focused on gathering information in support of the situation analysis. Server administrators are involved in this activity because inventories are collected centrally and if the organization includes several sites, must first be collected locally, and then assembled centrally.



An excellent source of information on inventory requirements and infrastructure preparation is the **Infrastructure Remediation Guide** of the **Business Desktop Deployment Solution Accelerator 2007**, especially its two appendices. This guide can be found at <http://www.microsoft.com/technet/desktopdeployment/bdd/2007/InfraRmdtn.mspx>.

The second inventory is discussed further below, but it is focused on the specific details of each system you intend to migrate.

The Inventory Assessment Tool

Ideally, an inventory system will have the ability to collect a variety of information from a variety of different sources. Sophisticated inventory systems are actually tied into asset management systems and while the inventory service is under the control of the server administrators, the inventory data is under the control of the Finance department of the organization.

A good inventory tool will have three key features:

- Hardware inventory
- Software inventory
- Reporting capabilities

Chapter 4 listed many more features for the inventory tool you select, but these three are the main focus of the tool. If you don't have an inventory tool in place, then you should rely on the guidelines list in Chapter 4 to identify what you need in this tool. Deploying an inventory tool falls directly onto the server administrator's plate because it is a central network service.

If you are a small organization and don't want to obtain a sophisticated tool, then you can look to free tools. There are tons of free tools on the market, but as you would expect, they require a bit of work to get the results you'll need. All you have to do to find them is to perform a search with your favorite search engine and you'll have a complete list. The organizations that use free tools will either be very small or have very simple networks that they are very familiar with.

Microsoft offers three free tools that provide inventory. You may have tested them out by now, but here they are again.

- The **Microsoft Windows Vista Hardware Assessment (WVHA)** tool which unlike other inventory tools, is designed to work from a PC and can scan networks of up to 5,000 PCs. The WVHA is in beta at the time of this writing and can be found at <http://www.microsoft.com/technet/windowsvista/deploy/readassess.msp> Eventually it will make its way to the Microsoft Web site and be available for a free download. WVHA is an agentless tool that scans any computer that you have administrative privileges over. Microsoft states that it can run on a PC and it should since it requires both Microsoft Word and Microsoft Excel (2003 or 2007 versions). Data is stored within SQL Server 2005 Express which is installed as you install WVHA. WVHA does not recognize the presence of a real version of SQL Server 2005 even if it is installed and will install the Express version anyway. All the more reason for leaving this tool on a PC. It does include a number of methods to collect information (see Figure 5.3) and once you get through the hype, especially in the Word reports, you actually get useful information.

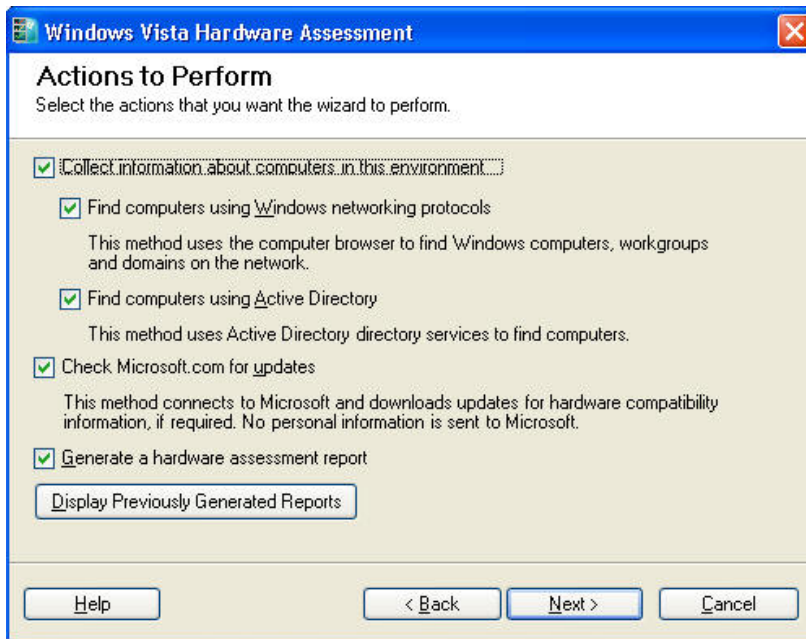


Figure 5.3. Using the Windows Vista Hardware Assessment tool

- The **Microsoft Software Inventory Analyzer (MSIA)** which is a graphical tool that scans local systems for a list of Microsoft products can be found at <http://www.microsoft.com/resources/sam/msia.msp>. MSIA will let you prepare a command line input file for the settings you want to use. Once again, administrator credentials are required, but output can be redirected to a network share. It only scans for Microsoft products, but at least it lets you find out which ones you have.
- The **Microsoft Application Compatibility Toolkit (ACT)** version 5.0 which is designed to provide an analysis of the applications running on your systems, whether they are used and their level of compatibility with Windows Vista. ACT can be found at <http://www.microsoft.com/downloads/details.aspx?FamilyID=24da89e9-b581-47b0-b45e-492dd6da2971&displaylang=en>. ACT requires a SQL Server database to run and as such should be installed on a server. In order to collect inventory, you need to prepare a collection package which must be run on each PC you want to scan. Administrative rights are required to run the installation of the package and since the package comes in .EXE format, it requires special approaches for delivery to the endpoints. Once delivered, the package runs on the local PC, collects information and then returns it to the central collection point. ACT is useful in that it lets you share information with a community of users through the Microsoft **Application Compatibility Exchange (ACE)**, though the value of ACE is only as good as the value of the input that goes into it. Since all input is anonymous, it may be questionable. Microsoft is trying to make it as valuable as possible, but its best value is focused on commercial software since few organizations will want to share information on their internally-developed applications. More on ACT will be discussed in Chapter 6.

Commercial tools also abound. For example, Symantec also offers a good inventory assessment tool for small to medium businesses. The **Symantec Ghost Solutions Suite (GSS)** version 2.0 consists of a console that can be located on either a PC or a server. Information on GSS can be found at http://www.symantec.com/enterprise/products/overview.jsp?pcid=1025&pvid=865_1. The console uses its own database. Agents must be delivered, again with administrative rights, to each target PC. Inventory tasks can then be performed from the console. Unlike other inventory systems, GSS does not run inventory tasks on a schedule; you need to tell it when to run. This way each time you collect the information, it is up to date.

GSS is not designed to cross routing boundaries or, in other words, wide area network (WAN) connections. If you have more than one physical location, you will need to install a GSS console into each site to collect the information for that site. There is no means, other than exporting data, to consolidate multiple inventories from multiple sites. GSS does however offer some very detailed inventory collections right out of the box (see Figure 5.4), especially for Vista Premium PCs, including items such as video memory. In fact, Ghost is the first tool to do so by default. Other tools require you to create a custom collection. Ghost is not strong on inventory reporting—contents have to be exported to a tool such as Microsoft Excel to create charts—but it is very strong on its traditional feature set: PC imaging and image deployment.

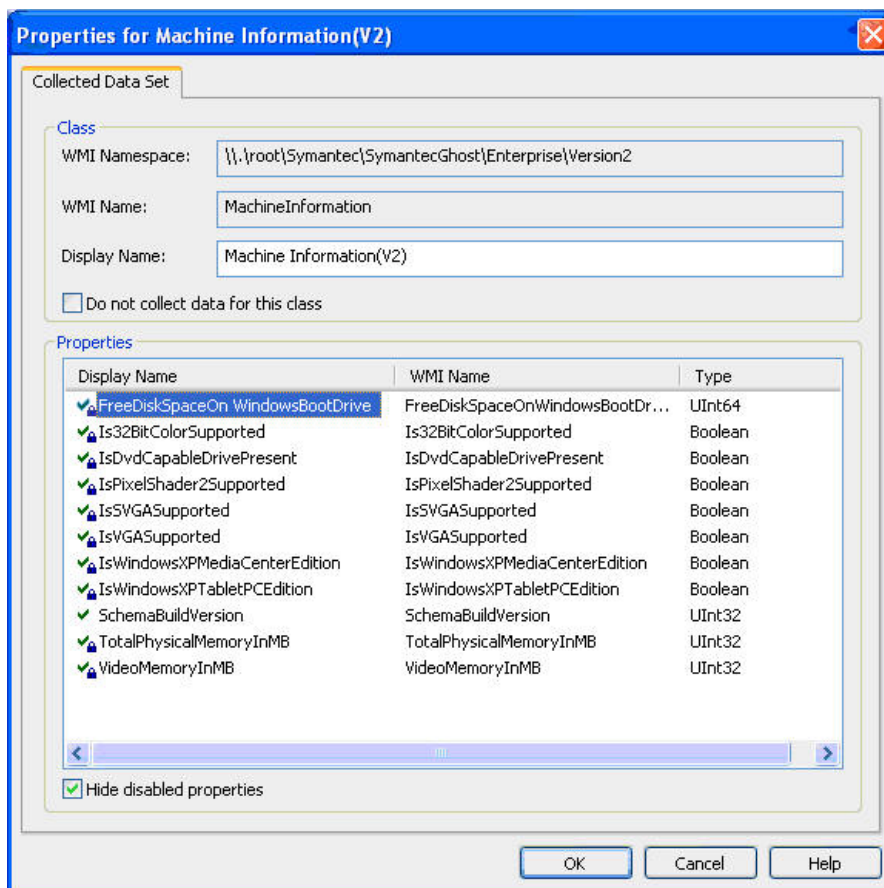


Figure 5.4. Ghost Solution Suite includes custom inventory collectors for Vista Premium PC readiness

Organizations that are using Active Directory might choose to rely on **Special Operations Software's Inventory** tool. Specops Inventory is the only tool that integrates directly with Active Directory to perform inventory collection and therefore does not require a secondary infrastructure to run (see <http://www.specopssoft.com/products/specopsinventory/>). It does however require a separate SQL Server database to store inventory data. Specops Inventory is quite powerful if your systems are all connected to the directory service and like Ghost, is really easy to set up and install since it relies on an infrastructure you have already deployed. Inventory collection is performed through the standard Group Policy client any Windows machine already includes. Just open an existing Group Policy Object (GPO) or create a new one, identify what you want to look for and close the GPO. Inventory will begin to be collected as GPOs are refreshed and applied. Reports are very easy to view since they rely on a Web interface.

Organizations that want to implement a full-fledged PC management system including inventory collection can look to three products:

- Altiris offers several different options for inventory support. The **Altiris Inventory Solution** (<http://www.altiris.com/Products/InventorySolution.aspx>) is specifically designed for inventory collection only. But, this solution is also integrated to different products. For example, the **Altiris Deployment Solution** is a full migration suite which also supports minimal inventory capabilities (<http://www.altiris.com/Products/DeploymentSolution.aspx>). The **Migration Suite** includes all of the components of the Deployment Solution plus Wise Package Studio for software packaging and software management as well as the full Inventory Solution (<http://www.altiris.com/Products/MigrationSuite.aspx>). The **Client Management Solution** (<http://www.altiris.com/Products/ClientMobile.aspx>) includes all of the above products as well as full lifecycle management of all client devices, not only PCs. Altiris has been one of the first software manufacturers to provide tools which support a migration to Vista. **Our recommendation:** if you are going for a full-fledged suite, then why not select the one that does it all and perform one single suite deployment.
- The **LANDesk Management Suite (LDMS)** is also a strong contender for Vista migration (<http://www.landesk.com/Products/LDMS/>). Like the Altiris products, LDMS provides full support for the PC Migration Cycle with special emphasis on Vista migration support. Inventories provide information on both hardware and software readiness while the other parts of the suite provide system imaging, profile protection and software packaging and deployment.
- Microsoft **Systems Management Server 2003 (SMS)** which is undergoing a name change in its next version to become System Center Configuration Manager 2007 (see <http://www.microsoft.com/smsserver/default.mspx>). Meanwhile, organizations that want to rely on SMS to support the inventory process should upgrade to service pack 3. SP3 is in beta as of this writing but should be released sometime in the first half of 2007. New features include better inventory reports for software inventory, reports for Vista hardware readiness and the ability to manage PCs running Windows Vista. In addition, SMS 2003 SP3 provides support for software rationalization by helping you identify applications with similar functionality, letting you consolidate on one single application for each functionality type, thus reducing costs and reducing migration efforts.

☞ Of all the products listed, only the products from Altiris, LANDesk and Symantec offer support for multicasting—the ability to deploy system images in one single data stream when deploying to multiple endpoints. This saves considerable bandwidth and time during deployments. Keep this in mind when making your choice.

Microsoft products will not have access to multicasting until the release of Windows Server Codenamed “Longhorn” later this year. At that time Microsoft will be adding multicasting capabilities to the Windows Deployment Services role Longhorn will support.

Technical Requirements for Inventory Tools

Every product that is oriented towards systems management uses the same basic framework. Data is always stored in a database, either SQL Server or other, servers are always required centrally to manage the multiple functions of the suite and secondary role servers are required if remote sites are part of the picture. Depending on the size of the organization, secondary databases may be required to collect information in remote sites and then replicate it to the central site, but this situation usually only applies to LORGs.

For deployment support, a central repository is required and once again, if remote sites exist, secondary repositories will be required. Data for inventories is collected from the remote sites and sent to the central site. Data for software and operating system repositories is provisioned centrally and replicated to the remote sites. Status of the deployment jobs is sent from remote sites to central repositories. This means that bi-directional replication technologies as well as bandwidth control technologies are required in the management solution. Finally, an agent is required on the PCs to communicate with the management service and perform management operations locally.

The overall solution will also need to take into consideration the management and administration of Windows Vista. Event log management is different in this OS as is Group Policy support. License management is also different. Server administrators will need to keep all of these considerations in mind when addressing the requirements for the migration (see Figure 5.5).

☞ **Our advice:** Start in the lab and then build out your systems management product deployment. Learn its features and then and only then, deploy it to production to collect your inventories.

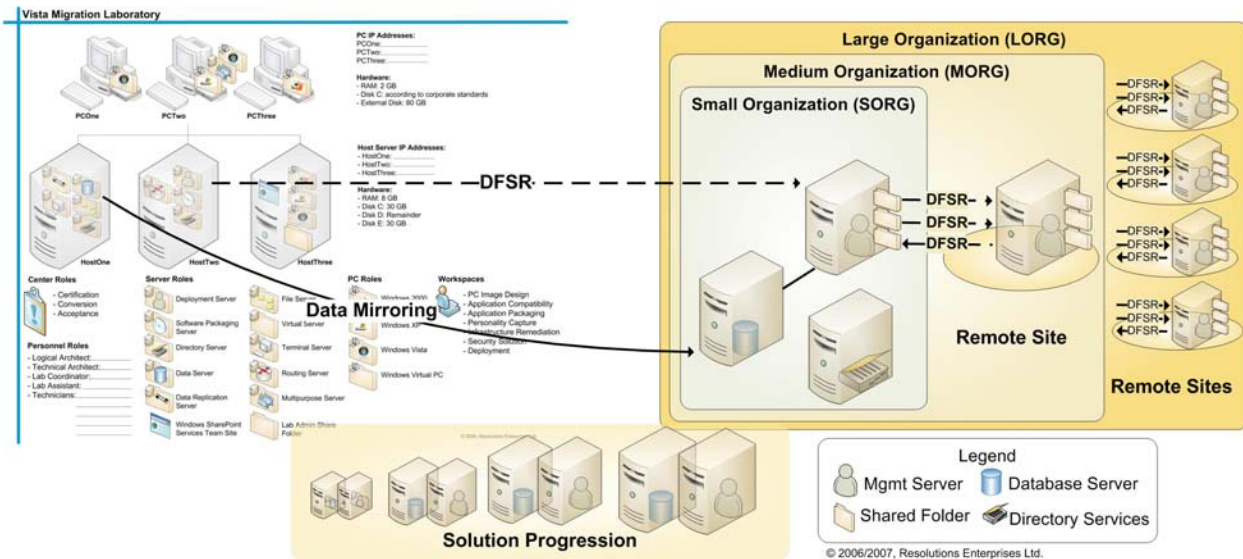


Figure 5.5. Infrastructure considerations in support of the migration

Procedures for the preparation of the infrastructure in support of the migration are outlined further in this chapter when we discuss the server preparation activities in the lab.

Collecting the Basic System Inventory

For the first inventory, you need to identify the scale of the deployment. This means you need to collect bulk data related to how many PCs you have in the network, what they have on them, which PCs meet which requirements and which PCs don't. Administrators will help collect this data from systems that are both online and offline, connected and not and provide it to the analysts which will help formulate the baselines for your migration.

The inventory collection process actually goes through a series of steps (see Figure 5.6):

1. **Collection:** Bulk information is collected from all of the systems in the organization.
2. **Data extraction:** Numbers and facts are drawn from the bulk information. These numbers and facts are sufficient to support initial project cost estimates and produce the business case for the migration.
3. **Refinement and additions:** A refinement process is applied to the original data to filter out unnecessary data and focus on more precise data—who is the principal user, what is actually used on the system, what needs to be recovered post migration and so on. Additional data may need to be collected to produce the required level of detail. For example, in order to determine if the applications found on the system are actually used by both the principal and other users of the system, an actual visit and discussion with the principal user may be required.
4. **Rationalization:** Rationalization processes are applied to bulk data to further refine the data. Three processes are required:

- a. **Reduce:** The objective of rationalization is to reduce the number of applications that will be carried forward during the migration. Be strict and remove anything that is not necessary. This means any duplicates in terms of functionality—only one drawing tool, only one word processor, only one browser, and so on—as well as multiple versions of the same product. Any deviations should require serious justification.
 - b. **Reuse:** Learn to reuse systems as much as possible. One of the best ways to do this is to standardize on all aspects of the solution—standardized procedures, standardized PC images, standardized applications, and so on. This will cut costs and ensure a more stable solution.
 - c. **Recycle:** If you have invested in some management efforts in the past, then focus on reusing as much as possible during your migration. For example, if you have existing Windows Installer packages, look to their conversion instead of rebuilding them. Aim to adapt systems instead of reinventing the wheel.
5. **Net values:** Net values are produced after all of the refinements have been applied.
 6. **User data sheets:** User data sheets are produced for each PC to be migrated. These sheets include everything that is now on the PC and everything that should be ported once the PC has been migrated.
 7. **Release management:** User data sheets are provided to the release manager. The release manager will produce the migration schedule from this information—information which will also be provided to the technicians that perform the migration.

This process is essential to the success of the migration as the hand off to release management is the driver for the actual migration. Remember, users are only happy if everything is as smooth as possible for them. This means that if you know items are going to change, make sure you integrate these changes into your communications plan and announce them well ahead of time.

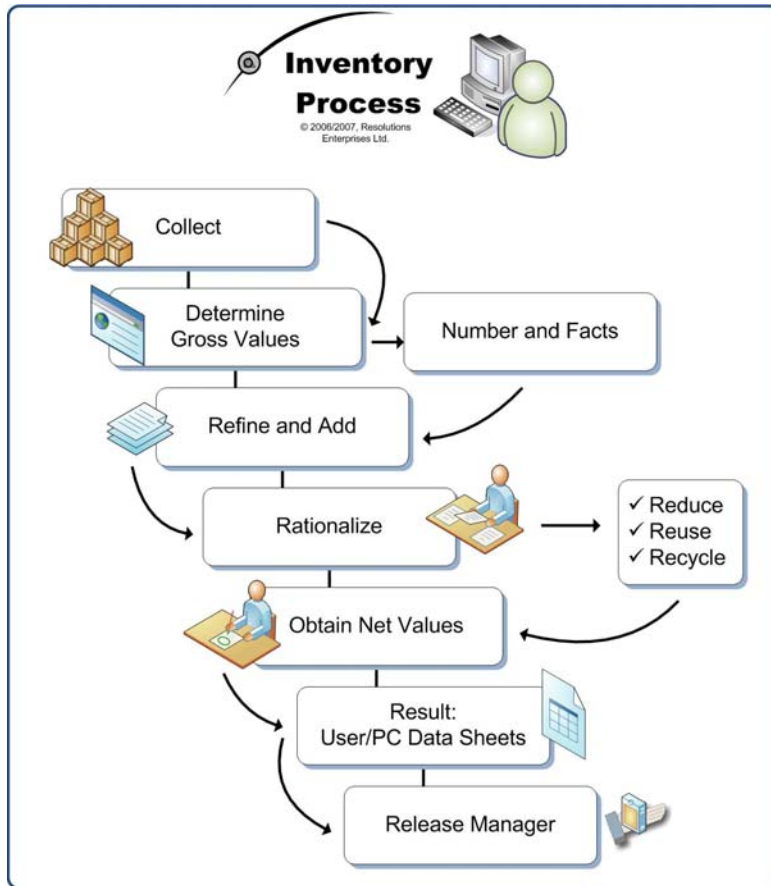


Figure 5.6. The Inventory Collection Process

As identified in the inventory process, information from the initial inventory analysis is aimed at identifying bulk values. The specific questions you need answered are:

1. How many desktops are in the organization?
2. How many laptops are in the organization?
3. Which PCs—desktops and laptops—need upgrades and how much do the upgrades cost?
4. How many PCs per user do you have? Will you carry over the same ratio with Vista?
5. How many applications are in the network?
6. How many of these applications will need to be carried over into the deployment?
7. Where are the PCs located?

These core questions help your team determine how much effort is required to perform the migration and how much it will cost. Reports should ideally be Web-based and dynamic so that users with different levels of authority can access and view them easily. They should also include graphics if possible—charts and graphs that can easily be copied into Microsoft Word documents or PowerPoint presentations to augment the value of the message you need to convey. In fact, this should be part of your selection criteria for the inventory tool. It is the goal of the systems administrators to assist project staff in collecting this initial data, whether it means deploying a new tool or not. Ideally, you'll already have this under control.

Server-based Operations in the Lab



These activities are part of the **Understand** phase of the QUOTE System.

Once bulk inventories are captured, the project team has enough information to drive the project forward. This all occurs within the Question Phase of the QUOTE System. Then, once the business case is presented and approved, you'll move on to the Understand Phase. This is where server administrators will be called upon to assist in two major activities:

- The preparation of the central services the laboratory will rely on.
- The preparation of the logical solution design.

As outlined in Chapter 3, the testing laboratory should be relying on virtualization technologies. As such, the server team will be called upon to prepare the host servers that will drive the virtual machines as well as preparing any virtual machine that will act as a server in testing. If you already use virtualization technologies, you can start with the preparation of the core virtual machines that will seed all of the other servers required to support the testing. If you don't use virtualization technologies yet, you'll need to begin with their installation.

Build the Host Servers

Host servers should be beefy machines that have a lot of power since their main purpose is to run virtual machines. This means lots of RAM, lots of disk space and several processors, ideally multi-core processors. The server hardware should also be 64-bit if possible as it will give you access to more memory than a 32-bit machine and it will let you create 64-bit virtual machines if you are using the right virtualization technology. Refer to Chapter 3 for the recommended configuration of the host server as well as for the virtual machines.

To prepare the host server:


1. Begin with the preparation of the server hardware, locating it in a rack if it is a rack-mounted server or in a blade casing if it is a blade server. Smaller shops will use a tower casing. Connect all required components.
2. Install Windows Server 2003 (WS03) R2 Enterprise Edition. This edition lets you run up to four virtual machines running Windows operating systems for free as their cost is included in the license for the host server OS. Remember to create three disk volumes:
 - a. C: drive with 30 GB for the OS.
 - b. D: drive with the bulk of the space for data.
 - c. E: drive with 30 GB for volume shadow copies.



Replace WS03 with "Windows Server Codenamed Longhorn" once it has been released, especially the version that includes Windows Virtualization. This version is the ideal Windows operating system for host servers.


3. Prepare the server OS according to your standard configurations. Make sure you update the OS and install anti-virus and backup software.

4. Configure Volume Shadow Copies (VSS) for drive D:. Place the shadow copies on drive E: and use the default schedule. Shadow copies protect any data that is on shared volumes. Since the D: drive is automatically shared as D\$ by the system, the data it contains is shared by default. For information on how to configure shadow copies, look up **10-Minute Solution: Using Volume Shadow Copy** at <http://www.reso-net.com/download.asp?Fichier=A64>.

 If, by the time you're reading this, Microsoft has released System Center Virtual Machine Manager (VMM) and you want to use Microsoft virtualization technologies in your lab, then rely on this tool instead of Microsoft Virtual Server because VMM can deploy Virtual Server without requiring the installation of IIS. More information on VMM can be found at <http://www.microsoft.com/systemcenter/scvmm/default.mspx>.

5. Install the virtualization software. If you're using Microsoft Virtual Server 2005 R2, then you'll need to install Internet Information Services first; remember this is done through adding and removing Windows components in the Control Panel. If you're using VMware server, then you just need to install that product.
6. Once the virtualization software is installed, you can begin to create your virtual machines (VM). This basically uses the same process as with the installation of the host server. If you use multiple editions of WS03 in your network, you'll want to create at least two core VMs, one for the Standard Edition and one for the Enterprise Edition. Then, use these VMs as the seeds for every server role you need to configure.
7. Don't forget to copy the seed servers and run Sysprep on them to generalize the installation. This way you can use and reuse the machines as much as needed.

The original VMs should be created as soon as possible because Unit testers will need to have access to server technologies, most likely a multi-purpose server image that includes Active Directory, file sharing, a database server, deployment services based on the technology you choose to use and so on. Once these machines are ready, they should be loaded onto external USB hard drives and delivered to the testing teams—one of which will be the server team as there will be new server-based technologies and configurations to test.

 If you want to fast-track this aspect of your project, you can rely on virtual appliances—pre-built VMs that include all of the required features to support each testing level—that have been prepared by third parties. Go to <http://www.reso-net.com/livre.asp?p=main&b=Vista> to find out more about virtual appliances in support of the Desktop Deployment Lifecycle.

Build Central Laboratory Services

Now that some core VMs are built and other technical teams can go on with their work, you can begin to build the systems that will support both the project and the lab itself. These systems can be built inside virtual machines as they are protected by VSS and other backup technologies. The systems or server roles the lab and the project require include:

- A directory service which may be the same as your production directory. In most cases, it is best and easiest to create either a separate forest as you would in the case of all of the testing levels you need to use—Unit, Functional, Integration and Staging. But, for the laboratory’s own use, you might just create a separate domain within your production forest or just create organizational units (OU) inside your production domain. It all depends on the level of isolation you need for this project. **Our recommendation:** use a separate domain in your production forest. This will automatically create trusts between the production domain and the project domain so users can continue to work with their normal, production user account, but grant them different privileges within the project domain. This is something you cannot do when placing them in OUs within the same domain. Remember that you will need at least two domain controllers to protect the information contained in the domain.
- A database server which will be used to host data from a number of different technologies, namely the software packaging system, the management system, Microsoft’s Application Compatibility Toolkit if you decide to use it, Windows SharePoint Services and any other structured data the project requires. **Our recommendation:** install SQL Server 2005 SP1. SQL Server is a comprehensive database tool that doesn’t break the bank when you acquire it and will provide a series of different protection services for the data it stores. In addition, SQL Server 2005 SP1 supports data mirroring which will let you automatically transfer data from the lab environment to a production database server when you’re ready.
- A server running Windows SharePoint Services version 3.0 (WSS) which will be used to host the project’s collaboration team site. WSS can be found at <http://www.microsoft.com/downloads/details.aspx?FamilyID=d51730b5-48fc-4ca2-b454-8dc2caf93951&DisplayLang=en>. You will need to install version 3.0 of the .NET Framework in support of this tool. You can find a link to the Framework on the same page as the WSS download. To speed the preparation of the team site, upload the team site template from the companion Web site (www.reso-net.com/livre.asp?p=main&b=Vista) and follow the included instructions to load it into your WSS environment. Assign a WSS administrator to begin granting access to team members. Most members should be contributors while the project manager and the project assistant should be site owners. The lab coordinator and the lab administrator should be owners of the lab subsite. Data for this site should be stored in the SQL Server you prepared earlier.

This should be enough to get the project and the technical teams going at this stage.



Note: All project documentation—plans, presentations, communiqués, technical documentation, training materials, everything—should go into the SharePoint team site and should be protected by proper backup technologies and systems as well as proper security settings. In addition, technical tasks should be drawn out from the project plan and should be assigned to team members on the site. This will give you an excellent tool for tracking project progress as well as storing all project data.

Participate in the Solution Design

The server team also needs to provide support to the design of the solution the project will implement. As outlined in Chapter 2 and in the QUOTE System, you begin with a logical solution design, focusing on the new features of the technology you will implement to draw out how your organization will benefit from them. This is done by examining several sources of information: help desk logs for the most common problems, new feature information for the technology to be implemented, industry sources for best practices and recommendations and so on.

The server team will focus on anything that is centrally based and that will provide enhanced support for the new technology. This involves items such as modifications to existing infrastructures, not in support of the operation of the project, but rather in support of the migration itself and the operations the organization will need to perform once the deployment is complete. The items that need to be covered in this initial solution are outlined in the remainder of this chapter.

Prepare the Detailed System Inventory

The next step is to provide support for the collection of detailed inventories. Remember that the initial inventory was designed to provide bulk information. Now you need to assist the project in obtaining detailed information on each system to be migrated. One good place to start is with a detailed topology map of the network. Ideally, this map will identify which machines, printers, servers and switches are connected to each other. This will assist in the redeployment of the PC OSES as well as help determine if switches and routers are properly configured to support the deployment process. One great tool for this topology map is Microsoft Visio. Visio can generate topology maps from network scans and even better, can rely on Microsoft Baseline Security Analyzer (MBSA) to scan systems and then provide the information to Visio to generate the image of the network. The Microsoft Office Visio 2003 Connector for MBSA can be found at <http://www.microsoft.com/technet/security/tools/mbsavisio.mspx>.

At this stage you need to make sure you have inventory data for each and every system in the network either connected or not. This inventory needs to determine everything that will be required to rebuild the system as close to what it was as possible. One of the best ways to do this is to rely on User or PC Data Sheets. These sheets list everything about a system: applications, principal user(s), printer connections, optional hardware, peripherals and so on.



A sample User Data Sheet is available on the companion Web site at <http://www.reso-net.com/livre.asp?p=main&b=Vista>. New visitors must fill out a onetime registration to access these downloads.

Validating Inventories

In order to minimize the amount of work required to rebuild a PC, it is important to validate all of the content of the User Data Sheet. One of the most difficult items to validate is the list of installed applications. This is because many organizations do not use a proper application licensing strategy and will install applications on systems when needed, but never remove them when obsolete. In order to avoid reloading applications that are no longer required and in order to improve your licensing compliance once the project is completed, you want to validate this list as much as possible before you deploy the system.

One good way to perform this validation is to use a software metering system which monitors the use of software applications on each computer system. Applications that are not used are marked off and are not reinstalled on the migrated system. But, if you don't have such a tool, you'll need to validate the inventory with the principal user of the machine. This takes time and is best done by administrative staff that have been trained to understand what should and what shouldn't be on a system. The goal is to update the User Data Sheet as much as possible.

Rationalize Everything

The concept of rationalization has been covered several times before because it is a process that is vital to the success of the project. It will also greatly reduce project costs as it cuts costs in licensing as well as reducing the time to prepare and perform the deployment. The activities you need in support of this process involve the following:

- Define clear rationalization guidelines and rules.
- Commit to the rationalization guidelines and rules as a project.
- Obtain organizational, read 'management', buy-in to the rationalization process. There will be resistance and if you don't have this buy-in, you won't succeed.
- Prioritize software rationalization as much as possible. If your users have more than one machine, then also prioritize PC rationalization. With the advent of virtualization, there are very few reasons for having more than one system per user.
- Initiate a communications plan to all users on the benefits of rationalization. This will help reduce resistance.
- Request an initial inventory purge by all IS and IT directors. They will be able to identify obsolete systems immediately.
- Involve users and user representatives in the rationalization. They have their say and will be happy to be consulted.
- Request an inventory purge by users themselves. They often know best.
- Establish a User Representatives Committee (URC). The URC will represent users when contentions arise and will be the project's representative with respect to users.
- Obtain a Rapid Decisional Process from executives so that you can cut short any rationalization debate.

Once the inventory is validated, proceed through the rationalization process using the following guidelines:

- Remove all applications that are not actually installed on a PC.
- Remove server and administrative applications. They should be stored on servers and administrators should use remote desktop consoles to servers for this.
- Remove any non-PC applications.
- Remove multiple versions of the same application.
- Remove games and utilities such as music software or anything that is not corporate in nature.
- Remove all applications that will be replaced by the software kernel or the core image that will be installed on all PCs (for more information, see Chapter 7).
- Remove applications fulfilling the same function. This means one single drawing program, one single financial analysis program and so on.
- Identify number of users for each remaining application. This will help in the design of application groups and user roles.
- Identify value to business for each application that is retained. If value is low, remove it.
- Begin negotiation with users early. This is best done through the communications program.
- Ensure that an application and data conversion strategy is in place for rationalized applications. For example, if you are removing a drawing program, then you need to be able to convert existing drawings into the format of the retained tool.
- Ensure that software obsolescence and lifecycle guidelines are in place so that this does not have to be done again once the project is complete.

Once the list of applications, devices and peripherals has been reduced, you can move to the creation of groupings. For example, you should group applications into the following categories:

- Mission and business critical applications
- Common commercial applications
- Limited use packages
- In house applications
- Non standard hardware

These groupings will help structure how you manage these applications. Finally, use a risk management strategy to reduce the impacts of rationalization. This means:

- Prepare common applications first since you will be able to deploy them to the largest user base.
- Group role-specific applications into IT user roles and target the largest groups first.
- Keep limited use packages for the end of the deployment since their audiences are small.
- Do not provide conversion for applications that are not Windows Vista compatible; run them inside virtual machines running older OSes if they absolutely need to be retained.
- Provide shared virtual machines with older OSes for applications that users will not give up but are obsolete.

This strategy will help reduce the carryover from the existing to the new deployment.



The last two strategies are hard core and should be applied to anything you really want to get rid of. If you can't and you can afford it, convert the applications to Vista.

Perform the Inventory Handoff

Now that everything has been validated and approved, you are ready to hand off the User Data Sheets to the release manager. This hand off is critical because it controls how the deployment will be structured. The release manager will then use the network topology map along with the User Data Sheets to determine which sites will be deployed first and how each PC will be built. Ideally the information in the data sheets will have been input into a database that can help the release manager control the deployment. As the deployment occurs, this manager will need to select replacement users for deployment as targeted users are unavailable or don't show up for their portion of the migration activities.

Having a bank or pool of users that you can draw from during the migration will help maintain deployment rates and keep the project on time and on track. Otherwise, dates will slip as it becomes impossible to deploy as many PCs as targeted during each day of the deployment. This gets the release manager ready for the Transfer phase of the QUOTE System.

Perform a Profile Sizing Analysis

One other aspect of the migration that will be critical is personality protection. Remember that users will not be pleased if their favorite desktop background does not appear or they lose their custom Word dictionaries once they have migrated to a new OS. But profiles tend to be rather large and will require some form of protection during the migration. Because of this, server administrators must assist the personality protection team to determine where these profiles will be stored and how they will be protected.

Several tools today allow the storage of the profile on the local hard disk during the actual OS deployment. If you decide to use this strategy, then server administrators will have little to do here, but if you determine that you want to raise the quality assurance level of this process and you have enough bandwidth to do so, you should store profiles on a network location. There are several ways to do this.

The most common is to simply use the migration tool to copy the profile to a server before the migration, migrate the PC, and then restore the profile from the server once the migration is complete. Other strategies involve the use of technologies such as folder redirection or roaming profiles to protect user data. Whichever method you decide to use, if you choose network protection then two tasks will fall to server administrators:

- Estimating storage sizes for profile migration during the deployment and preparing network shares that can support these storage requirements.
- Implement a retention policy for the profiles where the profiles are backed up for protection, retained on disk for a period of time and archived once the time period runs out.

The retention policy quickly becomes a rotation policy that will prove essential if you do not want to find yourselves running out of space during the migration. You'll also want to look to creating local shares if you have remote sites and implement replication technologies to bring remote data back to central locations for long-term storage.



More on personality protection is covered in Chapter 8.

Perform Project Engineering Activities



These activities are part of the **Organize** phase of the QUOTE System.

While the Understand phase focuses on logical solution design, the Organize phase of the QUOTE System focuses on engineering tasks or the actual implementation of the solution. To date administrators have had the opportunity to test and play with different server-based technologies as affected by the deployment and the coming of a new PC operating system. Now, it is time to define how this solution will actually take shape. As such you now begin to implement several additional technologies, usually in the Integration and Staging test environments. This is one reason why documentation of each parameter and setting used to deploy the solution components is so essential at this stage.

You'll need to work on the following systems:

- **Support for the deployment/management tool:** Begin with at least one server running the management tool role. Depending on the tool you selected or even if you already have a tool, this process will allow you to learn how this tool will support your migration. Link this tool to the database server you created earlier. If you have multiple sites, you'll have to look to secondary servers for this tool if required. If you already have a management tool in place, then look to how it needs to be adapted—deployment of an upgrade or deployment of a service pack—to support the Vista migration.
- **Support for software installation:** Your project will need to choose whether you will be using traditional Windows Installer packages or whether you will aim for software virtualization or even a combination of both. This topic is discussed at length in Chapter 6. If you decide to use Windows Installer or MSI packages, then you will need a packaging tool. These tools require installation on a server, the creation of file shares in support of their use and linkage to a database server. If you opt for software virtualization, you'll find that these solutions usually require an agent on the PC and often rely on either server shares or server streaming services to deploy the applications. You can also choose both and use the packaging tool to integrate your applications to the software virtualization engine.
- **The Microsoft Application Compatibility Toolkit:** If you choose to use it, this tool will require installation on a server as well as linkage to a database. ACT collects information about applications, including usage information which can be quite handy in support of the rationalization process. Keep in mind that ACT works through the creation of packages in the form of executables that must be deployed and delivered to PCs. The PC package requires administrative rights for execution so you will need to come up with a solution for deployment. More on this is discussed again in Chapter 6.
- **File sharing services:** You'll need to deploy file sharing services, usually in the form of a file server which will be used to store vast amounts of information. Remember that it is always best to secure file shares through NTFS permissions than through share permissions. Required shares include:

- **Virtual machine source:** The source virtual machine images which must be shared as read only for technicians that want to access copies of the machines for testing on their own systems and read-write for server administrators that create and modify the machines.
- **Software installation media:** A source folder for software installation media. The lab coordinator and administrator should have read-write privileges and packaging technicians should have read privileges.
- **Software preparation:** A working folder for software packages where packaging technicians have read-write access. They use this folder as they prepare packages.
- **Software release:** A repository that is the official final repository of quality controlled software packages. Technicians should have read access and only the lab coordinator and administrator should have read-write access as they are responsible for the final release of these products to the project.
- **OS installation media:** You also need a source folder for OS installation media, updates and device drivers. The lab coordinator and administrator should have read-write privileges and imaging technicians should have read privileges.
- **OS custom media:** Imaging technicians will need a working folder for OS system images where they have read-write access.
- **Custom OS releases:** A repository where final OS image(s) are released. This should have the same access rights as the software release folders.
- **Data protection:** A folder with read-write access for personality protection technicians will also be required as they test out the tools they will use to protect profiles.
- **Unique namespaces:** Another useful technology organizations with multiple sites should include in the preparation is namespaces. Namespaces are very useful because they eliminate the need for customization inside the individual packages you will deploy. That is because namespaces such as those based on the Distributed File System (DFS), especially the DFS service from the R2 release of WS03, provide the ability to map to one single UNC name inside every single package no matter which site you are located in. That is because a DFS namespace uses a [\\domainname\sharename](#) format instead of a [\\servername\sharename](#) format when publishing shared folders. With DFS namespaces, you map this unique name to different targets within each site. This way, when a package needs to refer back to a server share either for installation or for self-healing or updates, it will always work. Namespaces are mapped to Active Directory and because of this are available in any site in the domain. They are much easier to work with than mapped drives because they always refer to the same name structure. The directory service is responsible for linking each endpoint with the appropriate target share, eliminating the possibility of error.

- **Replication services:** DFS, once again, the DFS service included in WS03 R2, also provides delta compression replication (DCR). This means that once shared folders are synchronized through an initial replication, DFS replication (DFSR) will only replicate modifications to any of the contents. If one single byte changes in a 1 GB file, then one single byte is replicated. In addition, DFSR is really easy to implement, taking literally less than five minutes to set up. If you have more than one site, you should definitely look to DFSR. It is included by default in any version of WS03 R2 and it just works. Linked with namespaces, it becomes a very powerful engine in support of migrations. Replications with namespaces should be set for:
 - **Custom OS releases** since they need to be available in all sites. Replication should be set one-way only from the lab's release folder to production servers. If multiple sites exist, replication should also go one-way from the central production site to all other sites.
 - **Software releases** since they will be required for the deployment. Once again, one-way replication from the lab to production servers is all that is required. If multiple sites exist, use the same strategy as for OS releases.
 - **Profile protection** should be captured from their location, stored on a local server and replicated to a central site for backup and protection. If a namespace is also used, then the profile protection scripts only need reference one single share name.

Both of these scenarios are provided by default in the File Server Management console of WS03 R2 (see Figure 5.7). Setting these scenarios up is very straight forward.

- **Data mirroring:** SQL Server 2005 SP1 offers data mirroring services which are pretty straightforward to set up. As the project proceeds, you'll find that there is data held within the various SQL Server databases that should be available in production. Using the data mirroring feature of SQL Server 2005 SP1, you can simply replicate this data from the lab to production servers. Data mirroring in this case is usually targeted one-way from the lab to the central production environment only.
- **Switch and router configuration:** In some instances, organizations modify the default settings of their switches and/or routers to block multicast traffic. Many network administrators do so to stop users from watching or listening to streaming feeds from the Internet. But, even if this is necessary, this traffic should be blocked only at the gateway to the Internet, not on the links to the internal network. Make sure your routers and switches will support the ability to stream multicasts to PC endpoints so that you can save considerable time and effort during your deployment as you should be using a multicasting tool for deployment. Or, if you can't or don't have access to their configuration, then select a tool that will rely on proxies to perform WAN multicasting, bypassing routers and switches altogether and keeping all multicasting traffic on the LAN.

These different activities will ensure that the deployment project has all of the server-based support it needs to complete smoothly. Other activities are also required, but these will be in support of operations, not deployment.

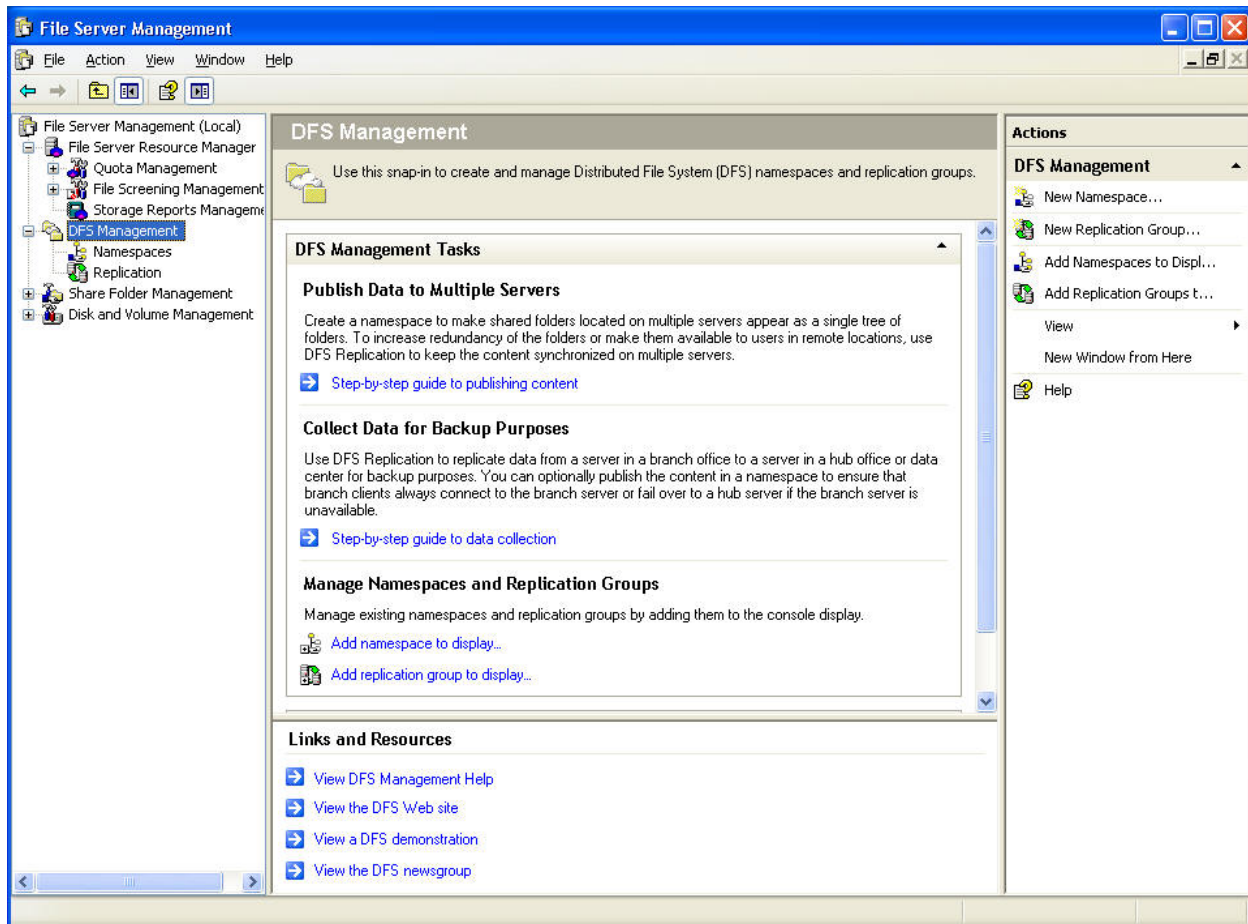


Figure 5.7. Creating replication scenarios in WS03 R2 is as easy as following a simple wizard

Vista OS Management Infrastructures

With Windows Vista, Microsoft elected to change and modify several different aspects of Windows management. Many of these will not be fully effective until Windows Server Codenamed “Longhorn” is released later this year. For example, even though the network access protection (NAP) client is built into Vista, Microsoft does not currently offer any NAP server service. But some of the technological improvements are available now. Active Directory can manage Vista Group Policy Objects (GPO), WS03 can manage folder redirection, WS03 can manage Vista licensing and you can take advantage of some of the new security features built into the PC OS. These activities will require server administration assistance since they will impact central services.

Manage Vista GPOs

Any organization that has taken the time to design and deploy an Active Directory forest and domain structure within its network has already realized the power and potential of this tool. That's because AD is not only designed to provide authentication and authorization as was the domain in Windows NT, but it is also designed to provide a complete infrastructure for the management of users, groups, printers, servers and PCs. All of these objects are managed through GPOs—directory objects that are designed to define the way a user's computing environment appears and behaves. GPOs were first introduced with Windows 2000 and are supplemented each time a new operating system (OS) or a significant update to an operating system is released. For example, Vista brings more than 800 new settings to Group Policy among other changes.



For best practices information on how to design an Active Directory for object management, download this free chapter from **Windows Server 2003: Best Practices for Enterprise Deployments** published in 2003 by McGraw-Hill Osborne at http://www.reso-net.com/Documents/007222343X_ch03.pdf.

With its extensive settings and controls, Group Policy provides an extremely powerful engine for the management of every aspect of a system's configuration from compliance to security baselines. GPOs can control registry hives, assign scripts, redirect data folders, deploy software and manage security settings. And, if you don't find the one setting you need to control, you can always add a custom administrative template to the mix and make your own modifications.

Most organizations using AD will use GPOs extensively, but will ensure that each GPO is designed to manage a single object type. This means that some will be designed to manage users, others will manage PCs and still others will manage servers. Segregating GPOs in this manner will not only improve the speed with which each GPO will be processed, but will also help in your delegation of administration structure.

Group Policy is an excellent vehicle for system administration, but it is possible to overdo it. Begin your Vista GPO strategy by inventorying the GPOs you have in place and then look them over to see if there is room for rationalization. Since Vista brings so many new settings, you don't want to find yourself in a situation where you are proliferating GPOs.



Microsoft provides a good tool to inventory Group Policy which can be found at <http://www.microsoft.com/downloads/details.aspx?FamilyID=1d24563d-cac9-4017-af14-8dd686a96540&DisplayLang=en>.



To learn how to rationalize the number of GPOs in your network while providing complete management services, download **Redesigning GPO Structure for Improved Manageability** at <http://www.reso-net.com/download.asp?Fichier=P73>.

While in previous versions of Windows, GPO processing occurred through the WinLogon process, in Vista, Group Policy processing has been decoupled from this process to run on its own, providing a more robust processing model. In addition, Microsoft has added several classes of objects that were previously difficult if not impossible to manage through GPOs (see Figure 5.7).

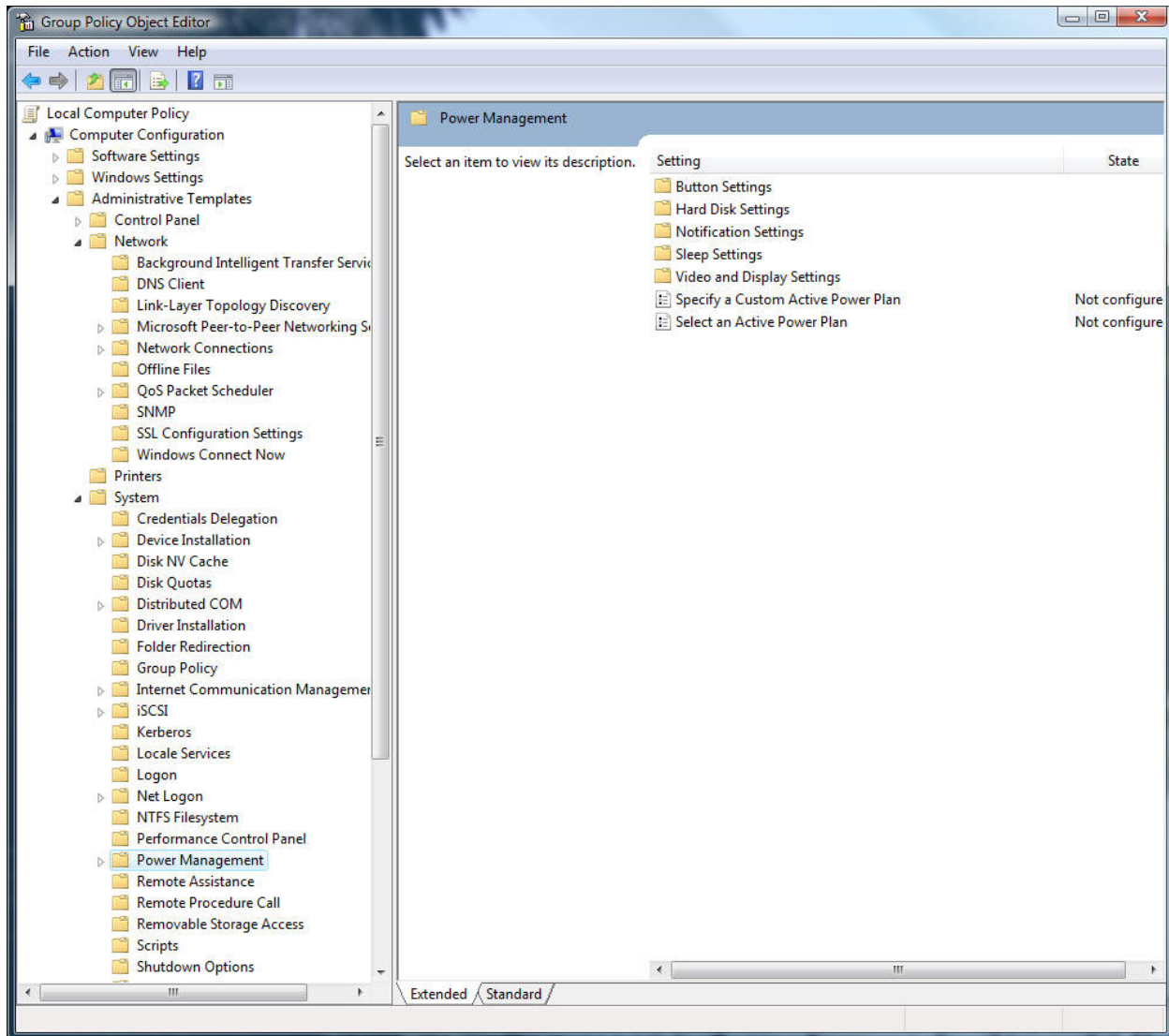


Figure 5.8. New GPO settings in Windows Vista

Some important new settings include:

- Device Installation to control whether or not users can plug in devices such as USB drives.
- Folder Redirection which has been vastly improved to protect a complete user's profile.
- Print Management which is tied to the WS03 R2 ability to publish printers through GPOs.
- Local Services which allow you to automatically change settings on PCs to match an employee's language settings.
- Logon and Net Logon to control the logon behavior.
- Power Management to help reduce the power consumption of PCs in the enterprise.
- User Account Control which lets everyone run with a standard user token.

- Wireless client controls to ensure that wireless connectivity conforms to organization policies.
- Windows Components including everything from Movie Maker to the Windows Sidebar.
- Windows Firewall which controls the state of the firewall both when connected to the internal network and when roaming outside the office.

There are many more settings. Take the time to review all of them and determine which ones should be set. Since these settings control mostly PCs, it will be the PC team that will identify which settings to apply along with recommendations from the server team. But one aspect of GPOs for Vista that affects server administrators is the new format Vista uses for administrative templates.



For guidance on deploying Group Policy with Vista go to <http://technet2.microsoft.com/WindowsVista/en/library/5ae8da2a-878e-48db-a3c1-4be6ac7cf7631033.msp?mfr=true>.

Prior to Windows Vista, all GPO definition templates used an ADM file format—pure text files that were organized in a structured manner. With Vista, Microsoft is introducing the ADMX format—a format based on the Extended Markup Language (XML) which provides much richer content for GPO templates. ADMX templates are now language independent, globalizing Group Policy settings. Each ADMX file is accompanied by one or more ADML files which include language-specific content. Global organizations will want to include an ADML file for each language their administrators work in. In addition, ADMX files can be centrally stored as opposed to the distributed approach used by ADM files—one on each domain controller in a particular AD domain. And, because of the increased number of policy settings in Vista, 132 ADMX files are included in the release version of Vista.

Because of the changes to Group Policy in Vista, the ADMX format is incompatible with the ADM format meaning that environments managing a mix of Windows 2000 and/or XP with Vista will need to either translate their existing templates to ADMX format or create new ones. Organizations that want to make sure critical settings are applied to all of their Windows clients will need to put in place a strategy that will support the translation of ADM to ADMX and vice versa, but of course, only for the settings that apply to any Windows version.




AMD/ADMX Conversion Tool

Microsoft licensed an ADM to ADMX conversion tool from FullArmor Corporation. This free utility is available at <http://www.fullarmor.com/ADMX-download-options.htm>.

While server administrators will not be involved as of yet with the conversion of ADM to ADMX templates, they will be involved with the creation of the central store for ADMX templates. In previous versions of Windows, each time a new ADM template was created it would be copied from the local system to the SYSVOL share on the domain controller. It would then be copied to every DC in the domain. With Vista, ADMX templates are referenced locally on the PC they were generated from, but if you have several PC administrators working on these templates, you'll want to create a central storage container that everyone will reference when working on new or existing templates. Creating a central store is easy, but it needs to be planned and performed by server administrators.

1. Log on with **domain administrative** rights.
2. Locate the **PDC Emulator** domain controller in your network. The easiest way to do this is to open the Active Directory Users and Computers console and right-click on the domain name to choose Operations Masters, click on the PDC tab to find the name of the DC. Then use **Explorer** to navigate to its **SYSVOL** shared folder. You use the PDC Emulator because it is the engine which drives GPO changes in the network.
3. Navigate to the **SYSVOL\domainname\Policies** folder where *domainname* is the DNS name of your domain.
4. Create a new folder called **PolicyDefinitions**.
5. Copy the contents of the **C:\Windows\PolicyDefinitions** from any Windows Vista PC to the new folder you created in step 4.
6. Include the appropriate **ADML** folders. For example, US English systems would use the en-US folder.
7. Launch the **Group Policy Editor** (GPEdit.msc). It will automatically reference the new central store as will all editors on any Vista PC in your domain.

Test this in the laboratory and then introduce the change to production when you begin the deployment.

 **Note:** There is no Group Policy interface for loading ADMX files into a GPO. If you want to add new settings based on an ADMX file, create the ADMX file and copy it to your central store. It will appear in the Group Policy Object as soon as you reopen the GP Editor.

 A spreadsheet listing all of the new GPO settings in Vista can be found at:
<http://www.microsoft.com/downloads/details.aspx?FamilyID=41dc179b-3328-4350-ade1-c0d9289f09ef&DisplayLang=en>.

Manage Vista Folder Redirection

As with former versions of Windows, Vista includes the ability to automatically redirect common user folders to central locations. This policy is much better than using roaming profiles because it will automatically reconnect users without having to download a vast amount of content and it is transparent to the user. In addition, Vista can localize the experience, automatically renaming common redirected folders into the appropriate language the user prefers. This means that folders such as Documents are named in the proper language when localization is enabled.

Other folder redirection enhancements include better synchronization. Vista includes a new synchronization engine that relies in delta compression replication—that's right, the same DCR that is available in WS03 R2 with DFSR. This provides a much better performance enhancement than with any previous version of Windows. These enhancements make folder redirection the best choice for protection of user documents and preferences. In addition, if you implement folder redirection with your launch of Vista, future migrations will make personality protection much simpler and easier than when profiles are stored locally.

Server administrators need to be involved in this activity because folder redirection relies on central folder shares. The biggest concern here is providing proper amounts of folder space for each user as well as making sure there is a strong backup and protection policy for these folders.

Manage Vista Security

There are several different aspects of security that you need to manage with Windows Vista—networking, wireless, User Account Control, and more—but one of the most important is the ability to run more than one local Group Policy Object on a system, up to three in fact. Vista applies these local GPOs in layers. As in previous versions of Windows, the first layer applies it to the computer system. The second applies it to a local group, either the Administrators or a Users group. The third can apply a local policy to specific local user accounts. This gives you a lot more control over computers that may or may not be connected to an AD structure.

The use of multiple local policies can make it easier to ensure that highly protected systems use different settings based on who is logging on, something that was a challenge in previous versions of Windows. To create multiple local GPOs, use the following steps:

1. Log on with **local administrative** rights.
2. Launch a new Microsoft Management Console using **Run, mmc /a**.
3. In your new console, go to **File, Add/Remove Snap-in**.
4. In the left pane, scroll down until you find the **Group Policy Object** snap-in and click **Add**.
5. For the first GPO which is applied to the local computer, click **Finish**.
6. **Add** another GPO snap-in.
7. In the Select Group Policy Object dialog box, click the **Browse** button.
8. In the Browse dialog box, click on the new **Users** tab (see Figure 5.9).
9. Select **Administrators** or **Non-Administrators** and click **OK**. Click **Finish** to add this GPO.
10. You can repeat steps 6 to 9, this time selecting a specific user account if you need to.

Edit each GPO setting as needed. Then, in order to apply these policies to multiple systems, copy them into the PC system image that you will be creating for these system types.

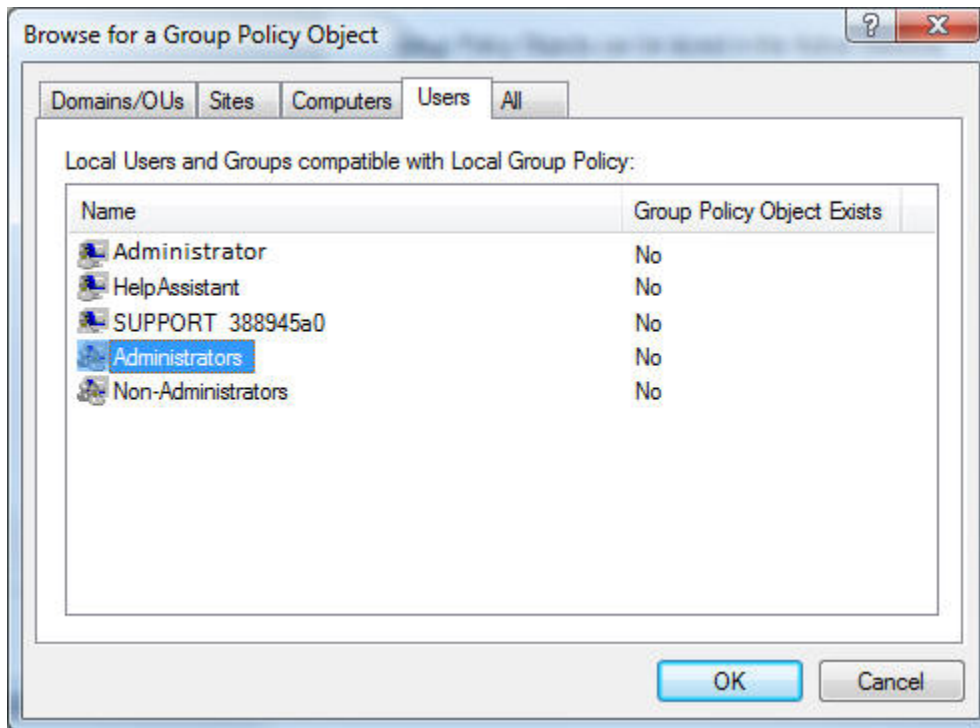


Figure 5.9. Applying a Local GPO to the Administrators group.

There is a lot of information related to Vista security and one of the best sources for this is the Vista Security Guide: <http://www.microsoft.com/downloads/details.aspx?FamilyID=A3D1BBED-7F35-4E72-BFB5-B84A526C1565&displaylang=en>.

Manage Vista Event Logs

The Event Log is one of the best ways to discover if anything untoward is going on in your system. And, if you're using Vista, you'll soon discover that its Event Log records a host of events that were unheard of in previous versions of Windows. In these previous versions, Microsoft used a number of different mechanisms to record events. Many products and sub-features of Windows recorded information in their own logs as if they didn't even know the Event Log existed.

It's no wonder that most administrators didn't even bother to verify any logs unless a specific event occurred or they were spurred on by others: security officers for example. It was just too much work. With Vista, most of these tools now record events properly and store them into the Event Log (see Figure 5.10). This is bound to make administration of Vista PCs easier, but of course, only when all your systems have been upgraded to Vista.

Vista's Event Viewer now categorizes events to make it easier to understand what changes have been performed on the system. Vista also provides detailed information on events, demystifying those arcane numbers and messages you could never understand. In addition, Vista can forward events to a central collector. Right now, that collector is another Vista PC since Windows Server Codenamed "Longhorn" is not released yet, but it is still a step forward.

Server administrators should be aware of these changes in preparation of the release of Longhorn Server. This is one reason why they should assist the PC operations team with Event Log configuration. This will get them ready for event management when Longhorn Server is released.

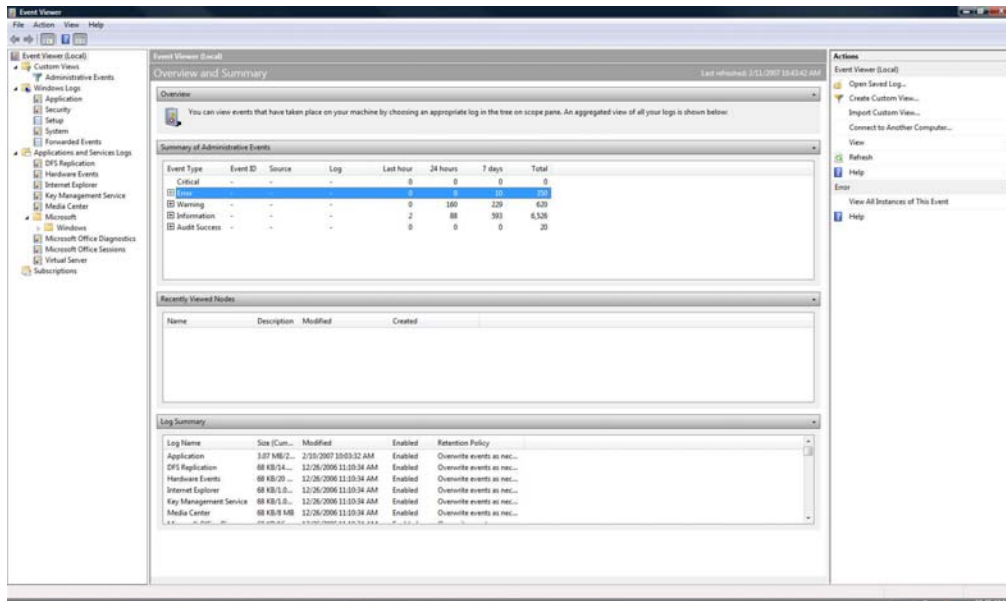




Figure 5.10. The Vista Event Viewer is rich with information.

Manage Vista Licenses

Organizations with volume license agreements with Microsoft will find they will need to implement a central Key Management Service (KMS) to activate and maintain Vista PC activation in their network. As mentioned in Chapter 2, anyone using a volume activation key (VAK) will need both activation and re-activation in order to maintain a proper level of user experience with the system. This protects volume activation keys in ways that have never been possible before. Organizations using multiple activation keys can also rely on KMS to provide activation services. The major difference between the MAK and the VAK is that the MAK requires only a one-time activation. The VAK requires constant re-activation (every 180 days). In addition, the MAK requires a communication with Microsoft at least through the proxy service if not from each machine using a MAK whereas VAKs never require access to Microsoft's activation Web site.

You can set up the Key Management Service on either Vista, Windows Server 2003 with SP1 or Longhorn Server. At the time of this writing, Longhorn Server was not available and, since you would not want to put this essential service on a workstation, Vista is not an option. Therefore, you should install this service on WS03 SP1. Make sure you run it on at least two servers to provide redundancy,

-  For more information on Volume Activation in general and to set up a KMS service, go to <http://www.microsoft.com/technet/windowsvista/plan/volact1.msp>.
-  To download KMS for WS03 with SP1, go to <http://www.microsoft.com/downloads/details.aspx?FamilyID=81d1cb89-13bd-4250-b624-2f8c57a1ae7b&DisplayLang=en>.

Support the Operations Team

As you can see, there are several different operations which need to be performed by server administrators in the Vista PC migration process. Several are outlined here and you will no doubt discover more as you work on your own migration project. This is why it is so important for the server team to take an active role in the outline, preparation, and delivery of the technical solution you will create to manage this new operating system.

Server team members should be ready to assist with any operation and should ‘audit’ non-server operations such as PC system image creation as this process will be carried forward to the coming Longhorn Server release. This will help give them a heads up for when it is their turn to deploy new technologies and new services.

In addition, server team members will be called upon to assist in the transition of project administration and operations procedures to production operations staff. If server team members participate early and eagerly in this process, then they can guarantee that there will be no administrative ‘surprises’ once the project is complete.

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>.