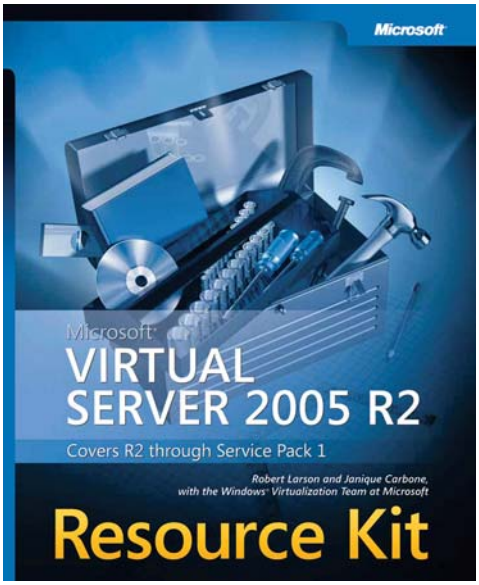

Microsoft® Virtual Server 2005 R2 Resource Kit

Robert Larson and Janique Carbone with the Windows Virtualization team

To learn more about this book, visit Microsoft Learning at http://www.microsoft.com/MSPress/books/10622.aspx

9780735623811
Publication Date: August 2007

Microsoft Press

Table of Contents

Chapter 4

Installing Virtual Server 2005 R2 SP1

In this chapter:

This chapter provides the information you need to install Microsoft Virtual Server 2005 Release 2 (R2) Service Pack 1 (SP1). It explains the differences in installing Virtual Server 2005 R2 SP1 on Microsoft Windows XP, Windows Vista, and Windows Server 2003. This chapter also covers a series of installation scenarios and shows how to interactively install Virtual Server for these scenarios, as well as how to use the command-line interface to perform the same tasks.

What Are the Prerequisites?

Before installing Virtual Server 2005 R2 SP1, review the requirements and prerequisites and make sure you have installed the required hardware and software to prevent failed installations. This section describes the minimum and recommended hardware and software requirements for installing Virtual Server 2005 R2 SP1. It separates the requirements into physical computer hardware requirements and operating system requirements. These requirements apply to all installation scenarios. Any scenario-specific requirements are discussed in the section that covers that scenario.

Hardware Requirements

The physical computer hardware requirements for Virtual Server 2005 R2 SP1 can vary widely from the minimum to recommended requirements. Table 4-1 lists the requirements for installing Virtual Server 2005 R2 SP1 to obtain a working system.

Important The minimum and recommended disk space and memory requirements listed in Table 4-1 are only for the disk space and memory required to install Virtual Server 2005 R2 SP1. These requirements do not include the disk space you will need for creating and storing virtual machines or the memory that you will need for running virtual machines. Planning and designing a Virtual Server host for different numbers and workloads of virtual machines will be covered in Chapter 15, "Virtualization Project: Planning and Design Phase."

Table 4-1 Virtual Server 2005 R2 SP1 Hardware Requirements

Item	Minimum requirement	Recommended requirement
CPU	1 CPU running at 550 MHz or faster	1 dual-core CPU running at 2 GHz or faster Intel VT or AMD-V enabled processor
RAM	256 MB	512 MB
Disk Space	60 MB	100 MB
Video	800 × 600 pixels or higher resolution monitor	1024 × 768 pixels or higher resolution monitor

Operating System Requirements

Virtual Server 2005 R2 SP1 comes in both 32-bit and 64-bit versions. To install the 32-bit version of Virtual Server 2005 R2 SP1, you must have a 32-bit host operating system installed on an x86-class server. To install the 64-bit version of Virtual Server 2005 R2 SP1, you must have a 64-bit operating system installed on an x64-class server. Virtual Server 2005 R2 SP1 does not support the Intel Itanium 64-bit processor line. Refer to Chapter 1, "Introducing Virtual Server 2005 R2 SP1," for a complete discussion of supported and unsupported hosts.

Supported 32-Bit Host Operating Systems

The following list is a summary of the supported host operating systems that can be used with the 32-bit version of Virtual Server 2005 R2 SP1:

- Microsoft Windows Server 2003 R2, Standard, Enterprise, and Datacenter Editions
- Microsoft Windows Server 2003, Standard, Enterprise, and Datacenter Editions with Service Pack 1 (SP1)
- Microsoft Windows Small Business Server 2003 with SP1 and R2 Editions
- Microsoft Windows XP Professional with Service Pack 2 (SP2)
- Windows Vista Enterprise, Business, and Ultimate Editions

Supported 64-Bit Host Operating Systems

The following list shows all the supported host operating systems that can be used with the 64-bit version of Virtual Server 2005 R2 SP1:

- Microsoft Windows Server 2003 R2, Standard, Enterprise, and Datacenter x64 Editions
- Microsoft Windows Server 2003, Standard, Enterprise, and Datacenter x64 Editions
- Microsoft Windows XP Professional, x64 Edition
- Windows Vista Enterprise, Business, and Ultimate, x64 Edition

Important Microsoft Windows XP and Windows Vista are supported only for nonproduction use as the host operating system.

Active Directory Requirements

Virtual Server 2005 R2 SP1 does not require Active Directory to operate. You can install Virtual Server 2005 R2 SP1 on a server in a workgroup and you will be able to create, modify, run, manage, and operate virtual machines on that host. When the Virtual Server service starts, it verifies whether the host is a member of an Active Directory domain, and if so it attempts to register service principal name (SPN) records with the Active Directory domain it is a member of.

Direct from the Source: Troubleshooting SPNs

To register SPNs, the user or group requires the Validated Write To Service Principal Name permission. By default, a user or computer account has this permission on its own Active Directory object. In addition, the Domain Administrators group has this permission on all objects. If you find that you are receiving errors in the Virtual Server event viewer that indicate failure to register SPNs or you just want to verify registered SPNs, you can use Setspn.exe to list or manually register SPNs for a machine running the Virtual Server service. Refer to Chapter 11, "Troubleshooting a Virtual Server Installation," for details on using Setspn to troubleshoot and register SPNs in Active Directory.

Allen Stewart
Program Manager, Windows Server Division

Installing Virtual Server 2005 R2 SP1 on servers that are members of Active Directory domains also allows you to reduce the management and operations of the Virtual Server installation. By joining an Active Directory domain, the security configuration and access control lists (ACLs) can use domain-based groups and users. This functionality allows you to establish a set of groups or specific user accounts that can be centrally managed but used across a pool of Virtual Server hosts in a server farm.

By combining standardized security groups on the Virtual Server hosts with domain global groups, you can establish a standard security configuration across the servers in the farm. If you try to maintain standardized security on each Virtual Server host that is not joined to an Active Directory domain, you will be required to create duplicate local user accounts, track and maintain separate passwords across the hosts, or establish poor practices such as synchronizing the passwords across the hosts.

Note Refer to Chapter 6, "Security in Depth," for a more in-depth discussion on the security features of Virtual Server 2005 R2 SP1 and how to best use them.

To take advantage of some features of Virtual Server 2005 R2 SP1, the host is required to be a member of an Active Directory domain. The Virtual Server service can then publish its binding information in Active Directory as a service connection point (SCP) object. This arrangement allows customers and independent software vendors (ISVs) to write scripts or applications to easily locate all instances of the Virtual Server service within an Active Directory forest.

What Are the Installation Scenarios?

During Virtual Server 2005 R2 SP1 installation, you select components that define how the Virtual Server operates and how it will be managed, choose optional tools to assist in managing the system, and determine how the security of the Virtual Server service is configured. Table 4-2 lists the available components.

Table 4-2 Virtual Server 2005 R2 SP1 Components

Component	Description
Virtual Server service	The Virtual Server service is a required component on any server where you want to define, create, and operate virtual machines.
Virtual Server Administration Website	The Virtual Server administrative interface is browser-based and therefore requires a Web server to host the Administration Website. The Administration Website can reside on the local server or on a separate server. The choice of where the Administration Website resides affects the security configuration of the Virtual Server service.
Virtual Server documentation and developer resources	The Virtual Server documentation and Component Object Model (COM) application programming interface (API) is required on any machine where you want to create, test, and run scripts or applications that will manage one or more Virtual Server hosts. This tool is typically installed with the Virtual Server service and on any development workstations where applications or scripts are being developed for Virtual Server.

Table 4-2 Virtual Server 2005 R2 SP1 Components

Component	Description
VHD Mount tool	The VHD Mount tool is required on any machine where you want to perform offline access to a virtual hard drive. This tool is typically installed with the Virtual Server service and consists of a client tool and a storage bus driver.
Virtual Machine Remote Control (VMRC) Windows client	The VMRC Windows client is required on any machine where you want to remotely manage virtual machines. This tool is typically installed with the Virtual Server service and independently on administrative workstations.

Virtual Server 2005 R2 SP1 comes in a self-extracting executable that contains a Microsoft Installer (MSI) package. As with most MSI packages, you have the option of performing a complete install or performing a custom install. Performing a complete install installs all available components on the local server. Selecting a custom install allows you to select components individually for local installation.

Note Virtual Machine Network Services (VMNS) and the Volume Shadow Copy Service (VSS) writer are also installed when you install the Virtual Server service. Virtual Machine Network Services provides the virtual network interface and handles all packet receipt and delivery with the virtual machines. The VSS writer provides a VSS-compliant backup interface for backup applications. You can see all installed VSS writers by using the *vssadmin list writers* command.

Table 4-3 provides a breakdown of the typical installation scenarios and a description of what is installed.

Table 4-3 Installation Scenarios

Scenario	Description
Upgrade	Upgrade all components from Virtual Server 2005 R2 to Virtual Server 2005 R2 SP1.
Single Server Installation	Install all components on the same server. Resources can be local or remote.
Central Administration Website Installation	Install all components except for the Administration Web Service on the Virtual Server host machine. The Administration Website is installed on a central server that is providing administrative services for one or more Virtual Server hosts. Resources can be local or remote to the Virtual Server host machines.
Documentation and Developer Resources Only	Install only the documentation and developer resources on the local machine to allow development of applications that make use of the Virtual Server COM API.
VMRC Only	Install only the VMRC client utility on the local machine to allow remote access to Virtual Server host machines.
VHD Mount Only	Install only the VHD Mount utility on the local machine to allow offline read/write modification of a .vhd file.

Configuring Constrained Delegation

When you select a complete install, you are installing all the components of Virtual Server: the Virtual Server service, documentation and development tools, VHD Mount utility, and Virtual Server Administration Website. If you will be accessing all of your resources—such as virtual hard disks, virtual floppy disks, and ISO images—from the local machine, there are no additional setup steps.

If you decide to install the Administration Website on a separate computer or need to access resources that are stored on a separate computer from the Virtual Server service, you have a security delegation requirement and additional configuration, called constrained delegation, is required in most cases.

Constrained delegation is the ability to specify that a computer or service account can perform Kerberos delegation to a limited set of services. This ability allows the user credentials to be passed from the Administration Website to the Virtual Server service or the server hosting the resources files, such as virtual hard disk (.vhd) files and ISO image (.iso) files, so that the user can access the files. In this scenario, you are required to use Integrated Windows authentication. Delegation does not work with Basic authentication.

Important Constrained delegation is supported only in Windows Server 2003 Active Directory domains in Windows Server 2003 domain functional level. This means that if your domain functional level is Windows 2000 mixed mode or Windows 2000 native, you must raise the domain functional level to Windows Server 2003 native level to configure constrained delegation. In order to raise the domain functional level to Windows Server 2003, you can only have Windows Server 2003 domain controllers; therefore, you must replace, upgrade, or remove any Windows NT 4.0 or Windows 2000 domain controllers that currently exist in the domain.

Constrained delegation is not supported when using Windows XP Professional or Windows Vista as the host operating system. If you install Virtual Server on a Windows XP or Windows Vista system, you will not be able to access resources on remote file servers.

Constrained delegation is configured from the Active Directory Users and Computers Microsoft Management Console (MMC) snap-in. When you configure constrained delegation, you need to know the machine that you want to delegate from and the server and services that you want to delegate to.

Important In a constrained delegation configuration, when a Kerberos token is passed from a source to a target configured for delegation, it maintains the original user requesting the action intact for complete auditing of user accounts.

In the scenario where you have the Administration Website on a computer separate from the Virtual Server service and the resources are local to the Virtual Server host, you need to dele-

gate from the Web server to the Virtual Server and select the Virtual Server service (VSSRVC) and Common Internet File System (CIFS) services for delegation. Figure 4-1 shows this scenario that uses delegation to one or more Virtual Server hosts.

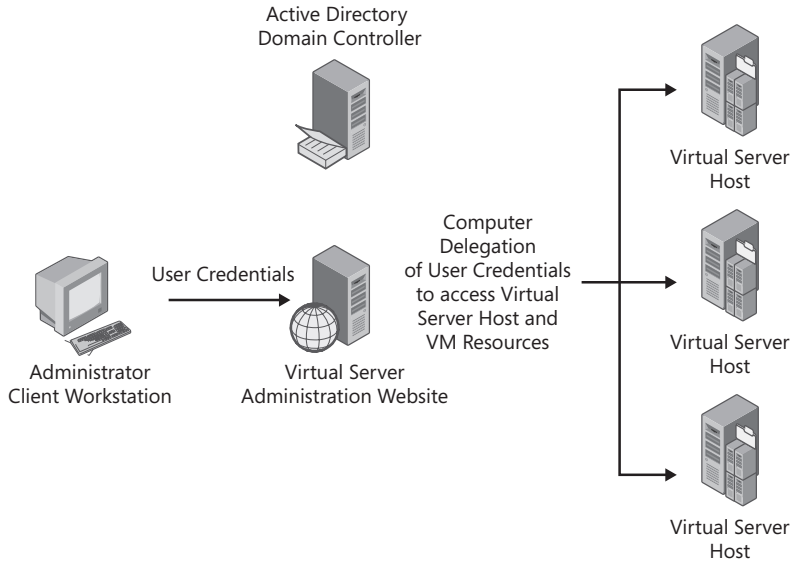

Figure 4-1 Delegation from an Administration Web server to a Virtual Server with local resources

If the virtual machine resource files are stored on a remote file server, you also need to delegate from the Virtual Server to the file server and select the CIFS service for delegation. Figure 4-2 shows this scenario that uses delegation to one or more file servers.

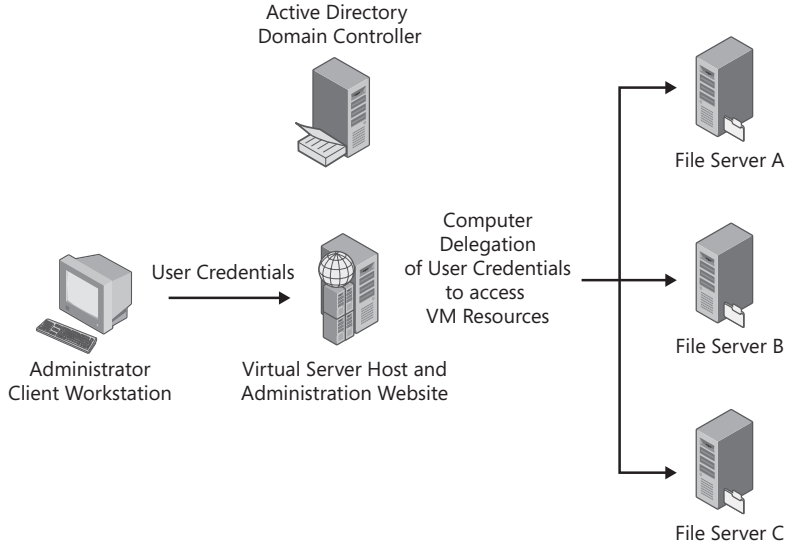

Figure 4-2 Delegation from Virtual Server to file server with remote resources

If the Virtual Server Website is installed centrally and the VM resource files are stored on remote file servers, you need to configure the following two separate delegations, as shown in Figure 4-3:

1. Delegate from the Administration Website to the Virtual Server hosts.
2. Configure a separate delegation from the Virtual Server host to the file servers, and select the CIFS service for delegation.

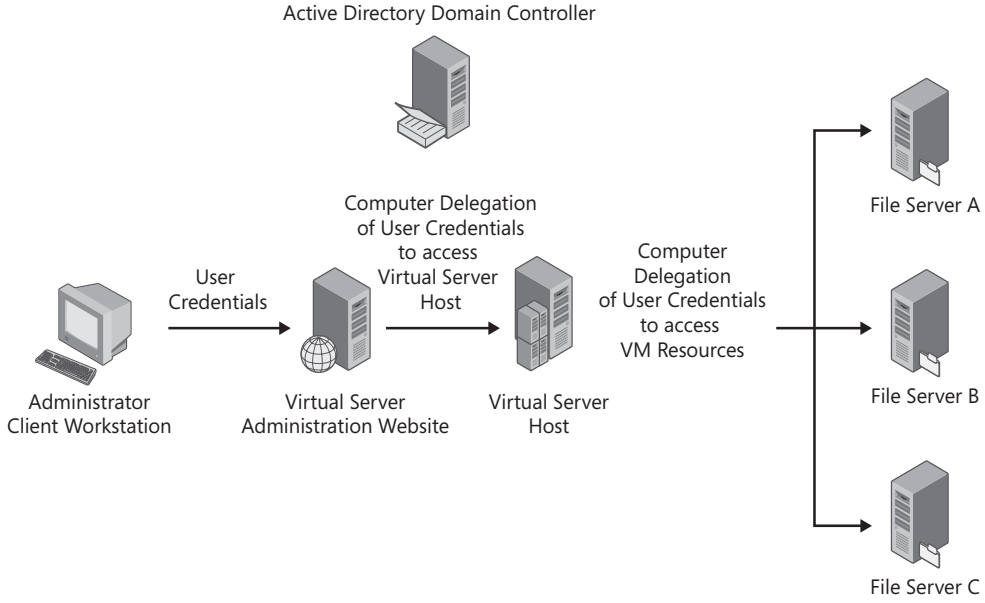

Figure 4-3 Delegation from Web server to Virtual Server and Virtual Server to file server

A constrained delegation configuration can get complicated. Keep detailed documentation on the computer delegations that you have set up and the services that were delegated. You will need this information to troubleshoot access issues and to manage the access in the event that a server is being retired or virtualized.

More Info For detailed steps for configuring constrained delegation, refer to Chapter 17, "Managing a Virtual Server Infrastructure."

Installing Microsoft Internet Information Services 6.0

Installing Internet Information Services (IIS) 6.0 requires slightly different procedures depending on the operating system. This section provides the procedures for installing IIS 6.0 on Windows XP, Windows Vista, and Windows Server 2003. This section is a reference for the three installation scenarios, and you should select the correct operating system procedure based on the operating system on which you are installing Virtual Server.

Windows XP

Installing IIS 6.0 on Windows XP is a simple process because this version of IIS has no configuration options to select from during install. IIS 6.0 on Windows XP supports only a single Web site and therefore will listen only on a single port. As with most Web servers, the default port is port 80.

Important Set the port for the default Web site before you install Virtual Server. Virtual Server will not allow you to change the port during installation. If you want to change the port of the Administration Website to something other than the default port 80 and you did not do so before you installed Virtual Server, you will have to uninstall Virtual Server, change the default port of the Administration Website using the IIS administrative console, and then reinstall Virtual Server.

Best Practices Standardize the port you use for Virtual Server Administration Websites. The default port for Windows Server 2003 installations is 1024. You should standardize on this port or select another standard and then use this port across all installations of IIS (Windows XP, Windows Vista, and Windows Server 2003).

To install IIS on Windows XP, follow these steps:

1. From the Start menu, select Control Panel.
2. Click Add Or Remove Programs and then click Add/Remove Windows Components to open the Windows Components Wizard, as shown in Figure 4-4.

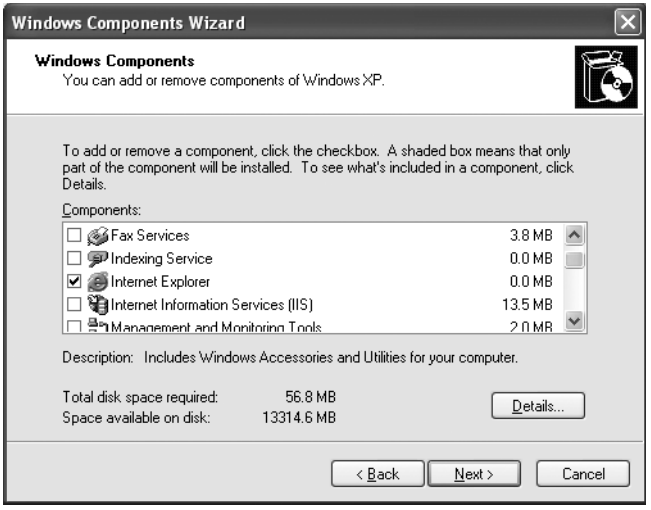

Figure 4-4 Windows Components Wizard

3. Select the Internet Information Services (IIS) check box to enable IIS for installation.
4. Click Next and the installation begins.
5. You might be prompted for the Windows XP or Windows XP service pack CD-ROM. Insert the CD-ROM in the CD-ROM drive and click OK.
6. When IIS installation is complete, click Finish.

Windows Vista

IIS installation on Windows Vista is an easy process, but selecting all the required components to support Virtual Server 2005 R2 SP1 Administration Website operation is not. Although you could take the simple approach and install all features under IIS, that would open your machine with new attack surfaces and is not a good security practice. The Virtual Server development team received feedback during beta testing that installing Virtual Server on Windows Vista was too error prone. To address this issue, the development team added the ability for the Virtual Server installation process to automatically configure the required IIS options. Although this configuration is done automatically, the steps to verify the IIS configuration are provided below.

Note If User Access Control is enabled, you will have to approve the launch of the Control Panel application because it requires administrative rights.

To verify that only the required features of IIS to support Virtual Server are installed on a Windows Vista machine, complete the following steps:

1. Log on to the Windows Vista machine with an account that has administrative rights.
2. Click the Vista Start button.
3. Select Control Panel to open the Control Panel page shown in Figure 4-5.

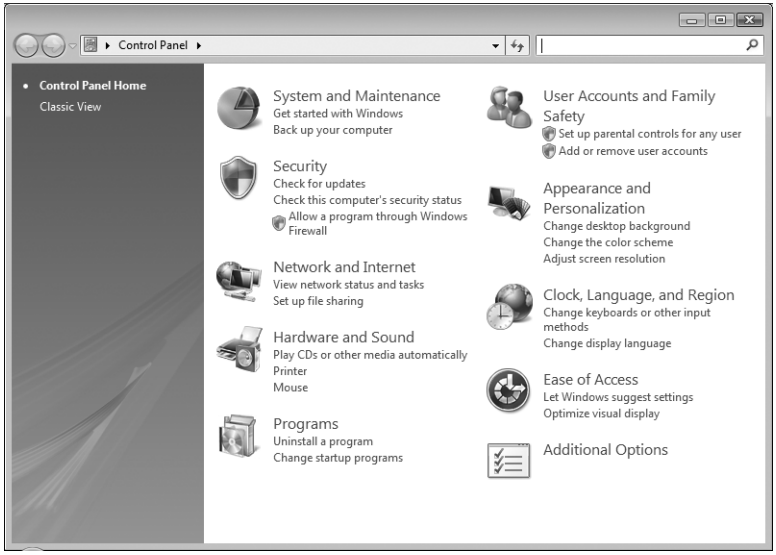

Figure 4-5 Control Panel

4. Click Programs to open the Programs page shown in Figure 4-6.

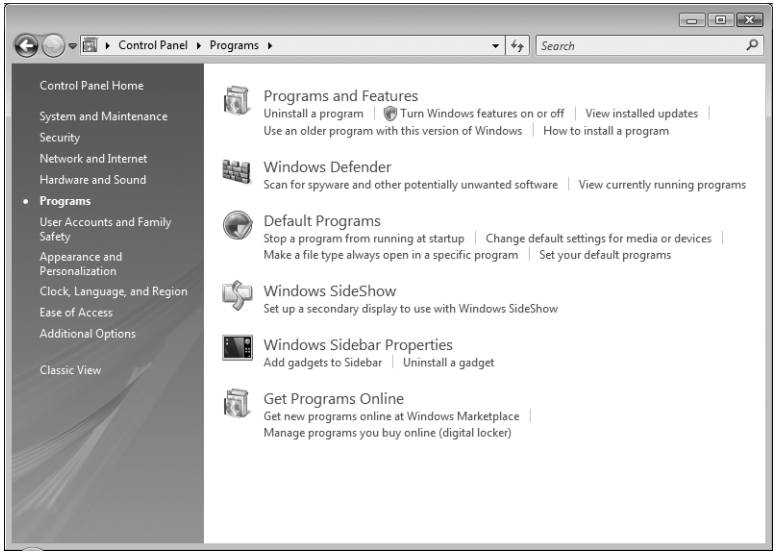

Figure 4-6 Selecting Programs from Control Panel

5. Under the Programs And Features option, click Turn Windows Features On Or Off to open the Windows Features dialog box shown in Figure 4-7.

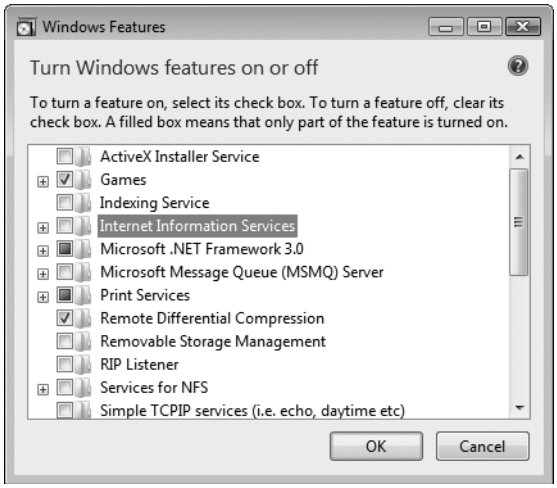

Figure 4-7 Windows Features dialog box

6. Expand the Internet Information Services node.
7. Expand the Web Management Tools node.
8. Verify that IIS Management Console is enabled.
9. Expand the IIS 6 Management Compatibility node.
10. Verify that IIS Metabase And IIS 6 Configuration Compatibility options are enabled.
11. Expand the World Wide Web Services node.
12. Expand the Application Development Features node.
13. Verify that CGI is enabled.
14. Expand the Common HTTP Features node.
15. Verify that the following options are enabled:
    - ❑ Default Document
    - ❑ Directory Browsing
    - ❑ HTTP Errors
    - ❑ Static Content
16. Expand the Health and Diagnostics node.
17. Verify that the following options are enabled:
    - ❑ HTTP Logging
    - ❑ Resource Monitor
18. Expand the Performance Features node.

19. Verify that the Static Content Compression algorithm is enabled.
20. Expand the Security node.
21. Verify that the Enable Windows Authentication feature is enabled.
22. Press OK to accept the IIS configuration settings.

On the Companion Media You will find a batch file on the companion media to automate the installation of Internet Information Services (IIS) on Windows Vista using the pkgmgr tool. The batch file is called Installiis.bat and is in the \Chapter Materials\Scripts directory.

Windows Server 2003

Installing IIS on Windows Server 2003 can be accomplished in two ways. The first way is similar to the Windows XP installation process and involves the use of the Add/Remove Windows Components option. Windows Server 2003 introduced a new interface for tasks like this through the Configure Your Server Wizard. This is a wizard approach for selecting server roles, and it greatly reduces the number of steps that it takes to install a role for a computer. Since the default options are the correct security options for Windows Server 2003, you can use the Configure Your Server Wizard approach.

To install IIS 6.0 on Windows Server 2003, complete the following steps:

1. From the Start menu, select Programs, Administrative Tools, and click Configure Your Server Wizard.
2. When the wizard starts, click Next.
3. On the Preliminary Steps page, click Next to open the Server Role page, which is shown in Figure 4-8. This page enumerates all network devices and connections that will be used during server configuration.

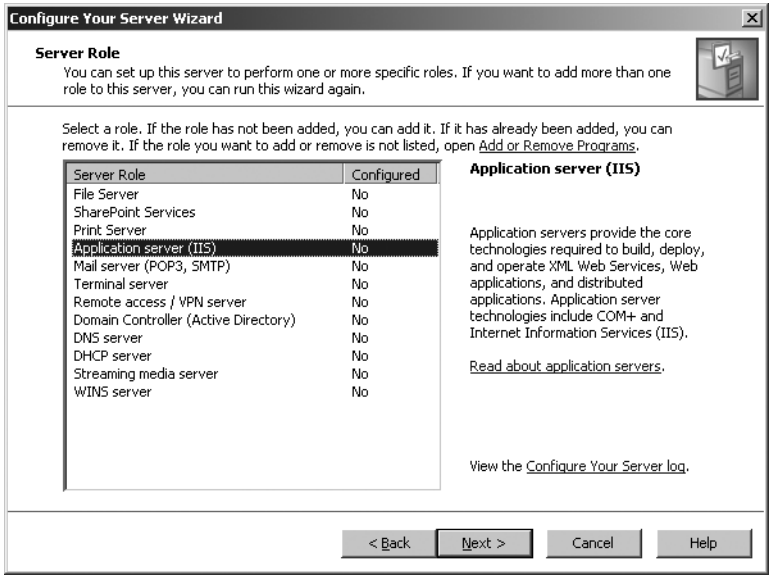

Figure 4-8 Server Role page of the Configure Your Server Wizard

4. Select Application Server and click Next.

   You will be prompted with an option to enable FrontPage Server Extensions and ASP.NET; however, you do not need either for the Virtual Server Administration Website to operate. Click Next.

5. On the Summary Of Selections page, shown in Figure 4-9, review the list of options that will be installed when you proceed, and click Next.

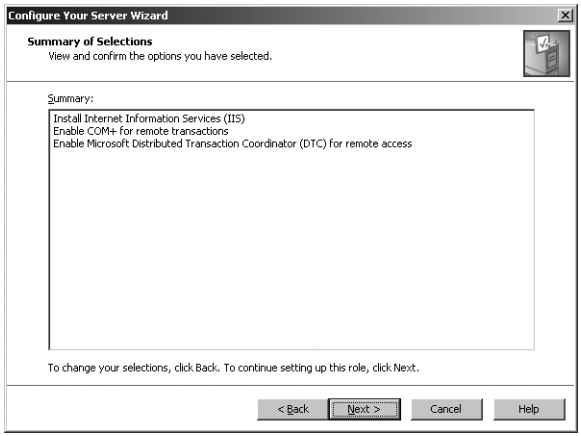

Figure 4-9 Summary Of Selections page of the Configure Your Server Wizard

The wizard scripts the installation based on the selections you made, and it uses that script to install the system in unattended mode. You will be able to see all the steps as the wizard proceeds. When the wizard completes processing, it displays a final page that declares that the machine is now an Application Server.

Installing Virtual Server 2005 R2 SP1

Depending on how Virtual Server will be used, the installation scenario could be an upgrade in place of Virtual Server 2005 R2 or could range from a simple single-server installation to a large multiserver farm of Virtual Server hosts maintained by a central Administration Website. Each installation scenario might require different components of Virtual Server to be installed on different servers, so the installation process supports custom installation and allows you to select any or all components. This section documents the procedures for the most common installation scenarios and important issues to watch out for during installation.

Note Although Virtual Server 2005 R2 SP1 can be installed on 32-bit or 64-bit versions of the supported operating systems, the procedures are the same for either version.

On the Companion Media On the companion media, you will find a directory called \Bonus Materials\Applications\Virtual Server 2005 R2 SP1. Inside that directory, you will find two subdirectories: \x86 and \x64. Each directory contains a single file, Setup.exe, for the associated 32-bit or 64-bit version of Virtual Server 2005 R2 SP1. This is the installation file for Virtual Server 2005 R2 SP1. You can install directly off the companion media, or you can copy the correct file version to the local hard disk and install from there.

Important The Virtual Server 2005 R2 SP1 installation process installs the Virtual Machine Network Services driver. When this driver is installed, it causes the host machine to lose access to the network. Make sure that the installation files are local on the server; otherwise, the installation may fail.

If you are using Remote Desktop to install Virtual Server 2005 R2 SP1 across the network, you will lose your connection while the driver is being installed, but typically it reestablishes the connection quickly. Make sure you use the /console command-line option with Remote Desktop when you establish the connection to the remote server.

Upgrading Virtual Server 2005 R2

Although Virtual Server 2005 R2 SP1 is labeled as a service pack, it is actually a full installation package that can be used to perform a fresh install or upgrade an existing installation of Virtual Server 2005 R2. The uninstall of Virtual Server 2005 R2 and the installation of Virtual Server 2005 R2 SP1 is fully automated in the upgrade process, so you do not have to uninstall Virtual Server 2005 R2 prior to installing Virtual Server 2005 R2 SP1.

Warning Virtual Server 2005 R2 SP1 required changes to the information stored in the save state (.vsv) file. Therefore, Virtual Server 2005 R2 saved states are not compatible with Virtual Server 2005 R2 SP1 save states. You must resume any virtual machines currently in save state and shut down the guest operating system cleanly before attempting the upgrade to Virtual Server 2005 R2 SP1. If not, you will have to discard the saved state before the virtual machine will power on.

To perform an upgrade of Virtual Server 2005 R2 to Virtual Server 2005 R2 Service Pack 1, complete the following steps:

1. Collect the following information before you start the upgrade:
   - The http port that the Administration Website is currently using
   - The Service account that the Virtual Server service is running under: Local System or Network Service
2. Open the Virtual Server Administration Website, and shut down all running virtual machines. Any virtual machine that is currently in saved state must be resumed from saved state and shut down.
3. Click the Start button, select Administrative Tools, and click Services.
4. Find the Virtual Server and the Virtual Machine Helper services, right-click each one and select Stop. This will stop both services and allow Virtual Server 2005 R2 SP1 to install.
5. On the companion media, obtain the correct version (32- or 64-bit) of Virtual Server 2005 R2 SP1 and launch Setup.exe to start the installation.
6. The dialog box shown in Figure 4-10 prompts you to verify that you want to upgrade the installed version of Virtual Server. Click Upgrade.

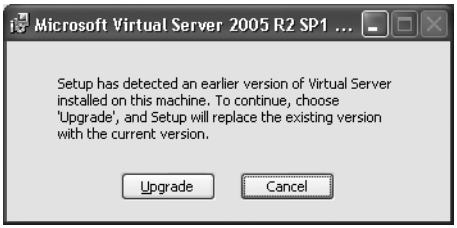

Figure 4-10 Verifying the upgrade

7. Click the Install Virtual Server 2005 R2 SP1 button.
8. Read the license terms, select I Accept The Terms Of This License Agreement if you agree, and click Next.
9. In the Customer Information dialog box, enter your User Name and Organization and click Next. The Product ID should be dimmed and already provided.
10. In the Setup Type dialog box, select the default option of a Complete Install and click Next.
11. Select the port that you want to use for the Virtual Server Administration Website, or use the default of 1024. Select the default option of Configure The Administration Website To Always Run As The Authenticated User, and click Next.

12. Accept the default to Enable Virtual Server extensions in Windows Firewall. This automatically enables firewall exceptions for the Virtual Server Web site and the VMRC protocol in the Windows Firewall. Click Next.
13. You have now selected all the configuration options for Virtual Server 2005 R2 SP1. Click Install to complete the upgrade.

You should see the upgrade proceed, and then you will see an Internet Explorer window that provides a summary of the installation and the links to the new Virtual Server Administration Website.

Single-Server Configuration

Installing Virtual Server on a single server is a typical scenario for environments where there is no security concern for IIS to be installed locally on the server or if there is a desire for each server to have local administrative capabilities. These procedures assume that no previous version of Virtual Server is installed on the server.

To install all Virtual Server components on a single server, complete the following steps:

1. Ensure that the server meets all the requirements for installation.
2. Install IIS using the procedures detailed in the "Installing Microsoft Internet Information Services 6.0" section of this chapter for the operating system version you are installing.
3. On the companion media, obtain the correct version (32- or 64-bit) of Virtual Server 2005 R2 SP1 and launch Setup.exe to start the installation.
4. Click the Install Microsoft Virtual Server 2005 R2 SP1 button as shown in Figure 4-11.

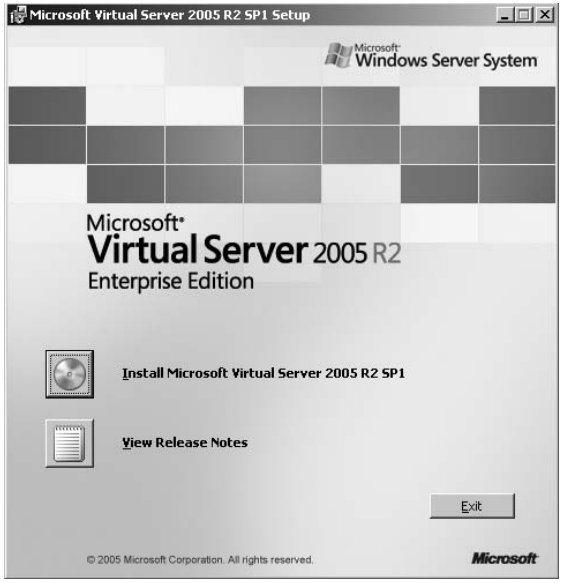

Figure 4-11 Starting the installation

5. Read the license terms, select I Accept The Terms Of This License Agreement if you agree, and click Next.
6. In the Customer Information dialog box, enter your User Name and Organization and click Next. The Product ID should be dimmed and already provided.
7. In the Setup Type dialog box, select the default option of a Complete Install. Click Next.
8. Select the port that you want to use for the Virtual Server Administration Website, or use the default of 1024, as shown in Figure 4-12. Select the default option of Configure The Administration Website To Always Run As The Authenticated User, and click Next.

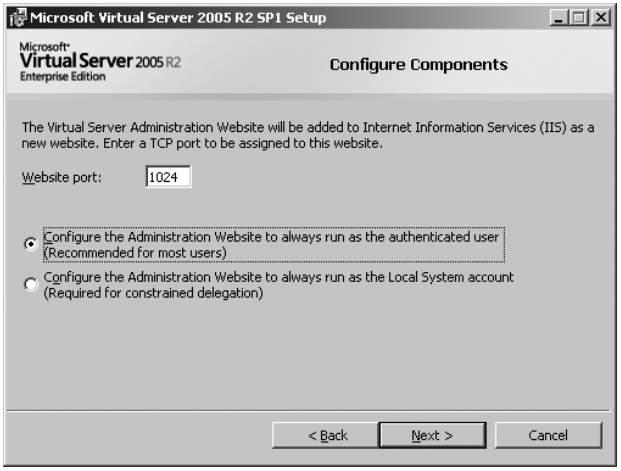

Figure 4-12 Configuring components

9. Verify that the Enable Virtual Server Extensions In Windows Firewall check box is selected as shown in Figure 4-13, and click Next. This automatically enables firewall exceptions for the Virtual Server Web site and the VMRC protocol in the Windows Firewall.

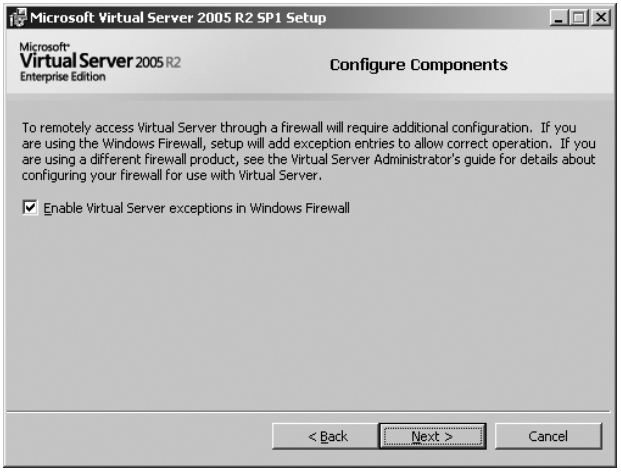

Figure 4-13 Enabling the firewall

10. Click Install to complete the installation.

You should see the installation proceed, and then you will see an Internet Explorer window that provides a summary of the installation and the links to the new Virtual Server Administration Website.

Local Administration Website and Remote Resources

In this scenario, you are installing the Virtual Server host and Website exactly like you would in the Single Server installation scenario. In addition, you must perform the constrained delegation configuration to allow the Virtual Server host to delegate the CIFS service to the file servers where the remote virtual machine resources are stored. The "Configuring Constrained Delegation" section in this chapter covers this scenario. Refer to Figure 4-2 for a diagram that depicts the configuration. The following instructions provide the detailed steps for performing that delegation. Perform these steps after you have installed Virtual Server for a single-server installation.

Note You must perform this step from each Virtual Server host to each file server that will store remote virtual machine files' resources. Therefore, if you have one host and three file servers, you will have to configure the delegation from the Virtual Server host to each file server for the CIFS service.

To allow the Virtual Server service to delegate a user's credentials to a remote file server for the CIFS service, complete the following steps:

1. On the domain controller, open Active Directory Users And Computers.
2. In the console tree, under Domain Name, click Computers, and then click the computer's organizational unit or the organizational unit in which the Virtual Server host is contained.
3. Right-click the Virtual Server host running the Virtual Server service, and then click Properties to open the Virtual Server host's Properties dialog box.
4. On the Delegation tab, select Trust This Computer For Delegation To Specified Services Only.
5. Select Use Any Authentication Protocol, as shown in Figure 4-14.

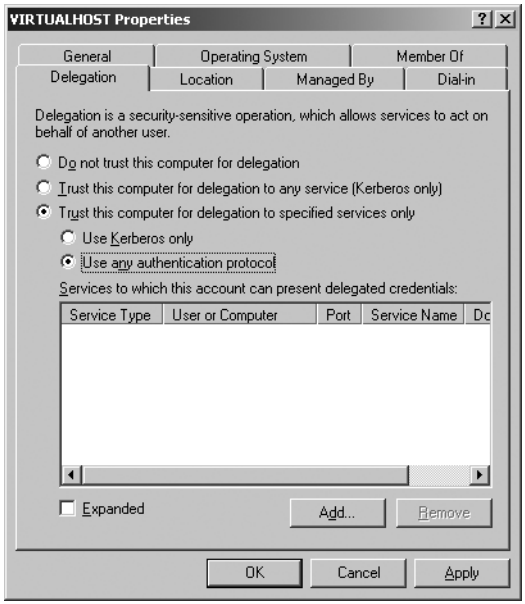

Figure 4-14 Virtual Server host's Properties Delegation tab

6. Click Add to display the Add Services dialog box, and then click the Users And Computers button.

7. Type the name of the computer on which the virtual machine resources are stored, and then click OK.

8. From the list of available services, select CIFS as shown in Figure 4-15, and then click OK. This selects the CIFS service as an approved service to accept delegated user credentials.

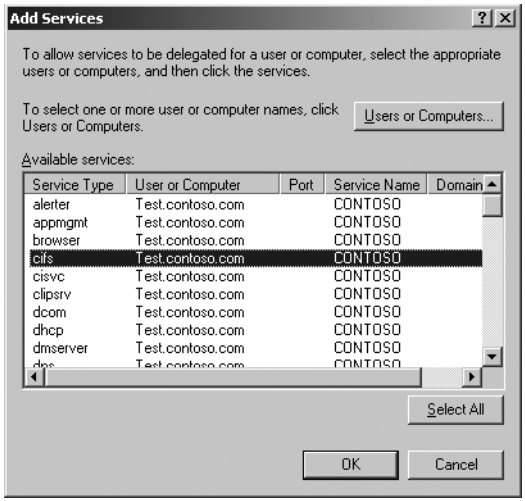

Figure 4-15 Selecting a service for delegation

9. If there is more than one file server that you need to delegate to, repeat steps 6 through 8 for each file server.
10. Click OK, as shown in Figure 4-16, to approve the Virtual Server host's ability to delegate user credentials to the CIFS service on the specified file servers.

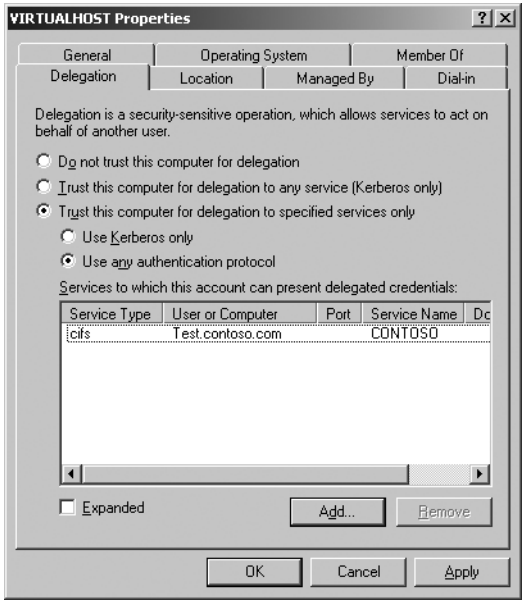

Figure 4-16 Virtual Server Properties Delegation tab

Server Farm with Central Administration Website and Remote Resources

In this scenario, you are installing the Administration Website on a central server to manage all the hosts in a server farm. You'll do this by installing each Virtual Server host with all services but the Administration Website and storing all virtual machine file resources remotely on one or more file servers. This is a typical data center installation scenario that provides a centralized administration point and increases the security of the Virtual Server host machines by reducing the attack surface, because IIS is not required on the host.

In this installation scenario, you must perform two constrained delegation configurations. The first is to allow the central Administration Website to delegate user credentials to the Virtual Server service (VSSRVC) for each host in the server farm. The second is to allow the Virtual Server host to delegate user credentials to the CIFS service running on the file servers on which the remote VM resources are stored. The "Configuring Constrained Delegation" section in this chapter covers this scenario. Refer to Figure 4-3 for a diagram that depicts the configuration. The following instructions provide the detailed steps for performing that delegation.

Installing the Administration Website on a Central Server

To install the Administration Website on a central server, complete the following steps:

1. Ensure that the server meets all the requirements for installation.
2. Install IIS using the procedures detailed in the "Installing Microsoft Internet Information Services 6.0" section of this chapter for the operating system version you are installing.
3. On the companion media, obtain the correct version (32- or 64-bit) of Virtual Server 2005 R2 SP1 and launch Setup.exe to start the installation.
4. Click the Install Microsoft Virtual Server 2005 R2 SP1 button.
5. Read the license terms, select I Accept The Terms Of This License Agreement, and click Next.
6. In the Customer Information dialog box, enter your User Name and Organization and click Next. The Product ID should be dimmed and already provided.
7. In the Setup Type dialog box, shown in Figure 4-17, select the Custom option and click Next.

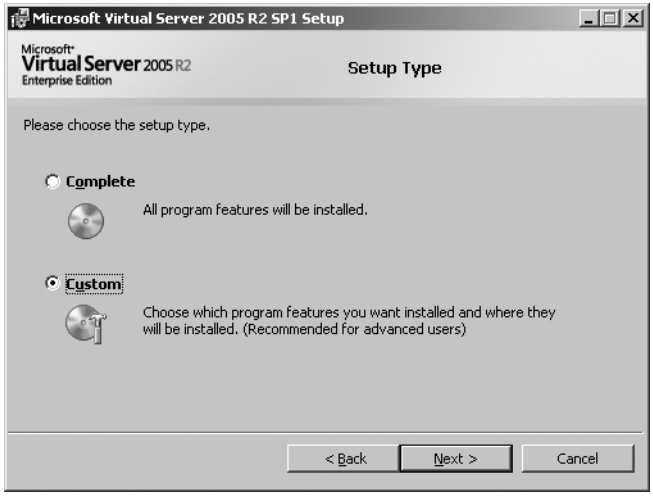

Figure 4-17 Setup Type dialog box

8. In the Custom Setup dialog box, shown in Figure 4-18, click Virtual Server Service, select This Feature Will Not Be Available, and then click Next. You do not want to install the Virtual Server Service.

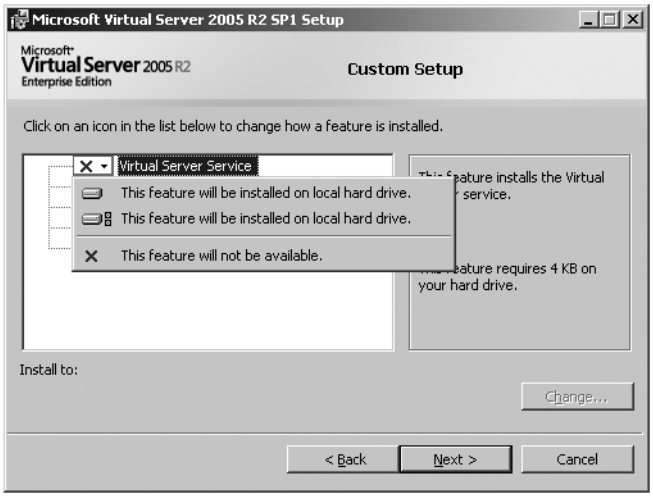

Figure 4-18 Disabling the Virtual Server service in the Custom Setup dialog box

9. In the Configure Components dialog box, shown in Figure 4-19, select the port that you want to use for the Virtual Server Administration Website or use the default of 1024. Select the Configure The Administration Website To Always Run As The Local System Account option, and click Next.

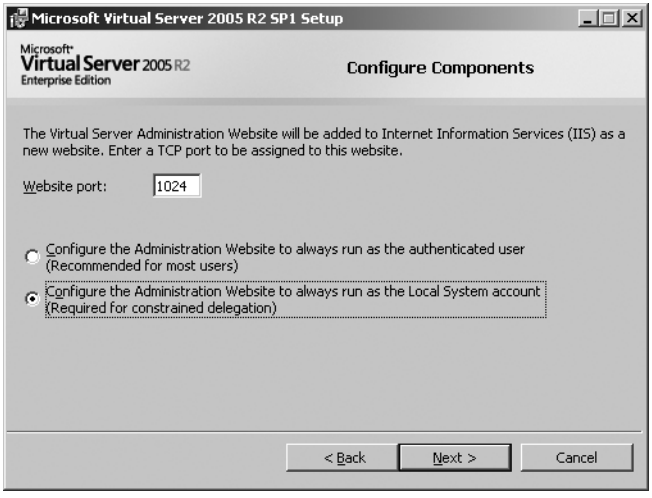

Figure 4-19 Configure Components dialog box

10. Accept the default to Enable Virtual Server Extensions In Windows Firewall, and click Next. This automatically enables firewall exceptions for the Virtual Server Web site and the VMRC protocol in the Windows Firewall.

11. Click Install to complete the installation.

You should see the installation proceed, and then you will see an Internet Explorer window display that provides a summary of the installation and the links to the new Virtual Server Administration Website.

Installing the Virtual Server Host Server with No Local Administration Website

To install the host server without a local Administration Website, complete the following steps:

1. Ensure that the server meets all the requirements for installation.

> **Important** Do not install IIS on this machine; you will not be installing the Virtual Server Administration Website and you do not require IIS.

2. On the companion media, obtain the correct version (32- or 64-bit) of Virtual Server 2005 R2 SP1 and launch Setup.exe to start the installation.
3. Click the Install Microsoft Virtual Server 2005 R2 SP1 button.
4. Read the license terms, select I Accept The Terms Of This License Agreement if you agree, and click Next.
5. In the Customer Information dialog box, enter your User Name and Organization and click Next. The Product ID should be dimmed and already provided.
6. In the Setup Type dialog box, select the Custom Install option and click Next.
7. In the Custom Setup dialog box, shown in Figure 4-20, click Virtual Server Web Application, select This Feature Will Not Be Available, and then click Next.

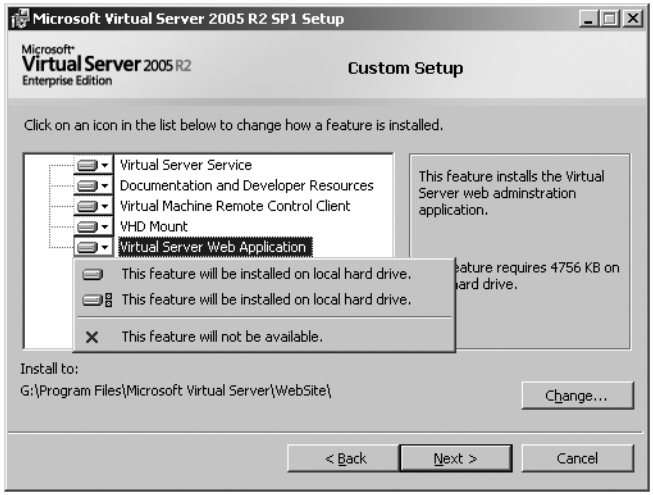

Figure 4-20 Disabling a Virtual Server Web application in the Custom Setup dialog box

> **Note** Because you are not installing the Virtual Server Web Application on this server, you are not prompted to configure the port for the Web server.

8. Accept the default to Enable Virtual Server Extensions In Windows Firewall, and click Next. This automatically enables firewall exceptions for the VMRC protocol in the Windows Firewall.
9. Click Install to complete the installation.

You should see the installation proceed, and then you will see an Internet Explorer window that provides a summary of the installation.

Documentation and Developer Resources Only

In scenarios where you need to perform development for Virtual Server, you might need to install only the development tools and documentation on a development workstation and none of the other services, such as the Virtual Server service or the Administration Website. You must have Virtual Studio or one of the Express development products installed on the development workstation before you install the development tools. Use the following instructions to install only the development tools and documentation.

To install the Virtual Server documentation and developer resources, complete the following steps:

1. On the companion media, obtain the correct version (32- or 64-bit) of Virtual Server 2005 R2 SP1 and launch Setup.exe to start the installation.
2. Click the Install Microsoft Virtual Server 2005 R2 SP1 button.
3. Read the license terms, select I Accept The Terms Of This License Agreement if you agree, and click Next.
4. In the Customer Information dialog box, enter your User Name and Organization, and click Next. The Product ID should be dimmed and already provided.
5. In the Setup Type dialog box, select the Custom Install option and click Next.
6. In the Custom Setup dialog box, shown in Figure 4-21, select each of the listed options except the Documentation And Developer Resources option, and select This Feature Will Not Be Available from the drop-down menu. Once you have disabled all components except Documentation And Developer Resources, click Next.

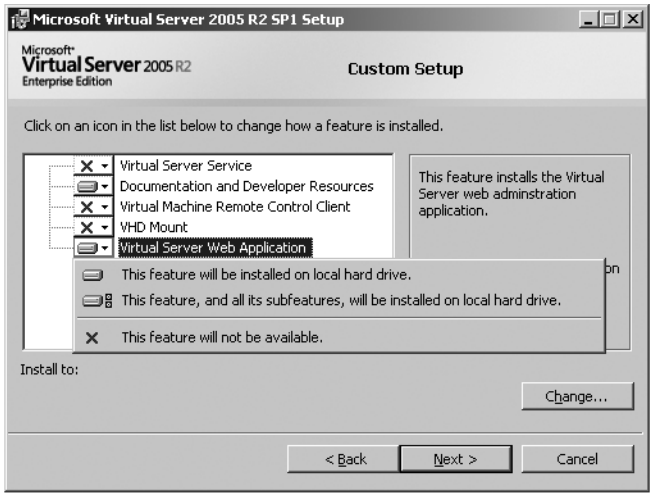

Figure 4-21 Installing Documentation And Developer Resources Only

7. Click Install to complete the installation.

You should see the installation proceed, and then you will see an Internet Explorer window that provides a summary of the installation.

Virtual Machine Remote Control Client Tool Only

In scenarios where you need to perform remote management of virtual machines, you might need to install the Virtual Machine Remote Control (VMRC) Client tool on an administrative workstation and none of the other services, such as the Virtual Server service or the Administration Website.

To install the Virtual Server VMRC tool only, complete the following steps:

1. On the companion media, obtain the correct version (32- or 64-bit) of Virtual Server 2005 R2 SP1 and launch Setup.exe to start the installation.
2. Click the Install Microsoft Virtual Server 2005 R2 SP1 button.
3. Read the license terms, select I Accept The Terms Of This License Agreement if you agree, and click Next.
4. In the Customer Information dialog box, enter your User Name and Organization and click Next. The Product ID should be dimmed and already provided.
5. In the Setup Type dialog box, select the Custom Install option and click Next.
6. In the Custom Setup dialog box, shown in Figure 4-22, select each of the listed options except the Virtual Machine Remote Control Client, and select This Feature Will Not Be Available from the drop-down menu. After you have disabled all components except the VMRC Client, click Next.

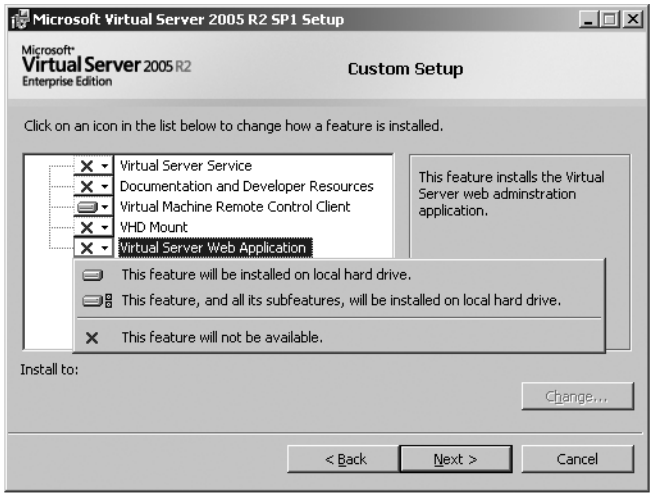

Figure 4-22 Selecting only the VMRC Client for installation

7. Click Install to complete the installation.

You should see the installation proceed, and then you will see an Internet Explorer window that provides a summary of the installation.

At this point, the VMRC client is installed into the C:\Program Files\Microsoft Virtual Server\VMRC Client\ directory. A Start menu program group is also created, and a shortcut to the VMRC client will be created. You should be able to launch the VMRC client utility from the shortcut in the menu.

Note The VMRC Client is a Windows application instead of a Web browser interface. The Windows VMRC Client actually uses the same ActiveX control as the Web browser version; it just has more features because it is a Windows application. For example, the VMRC client will allow you to expand the display to full screen and allow you to switch to other running virtual machines using the host key plus the left or right arrow keys.

VHD Mount Tool Only

In scenarios where you need to perform maintenance of virtual hard drive (.vhd) files or maybe offline modification of sysprep files in a virtual hard drive used as a template for provisioning new virtual machines, you might need to install the VHD Mount tool on an administrative workstation and none of the other services, such as the Virtual Server service or the Administration Website.

To install the Virtual Server VHD Mount tool, complete the following steps:

1. On the companion media, obtain the correct version (32- or 64-bit) of Virtual Server 2005 R2 SP1 and launch Setup.exe to start the installation.
2. Click the Install Microsoft Virtual Server 2005 R2 SP1 button.
3. Read the license terms, select I Accept The Terms Of This License Agreement if you agree, and click Next.
4. In the Customer Information dialog box, enter your User Name and Organization, and click Next. The Product ID should be dimmed and already provided.
5. In the Setup Type dialog box, select the Custom Install option and click Next.
6. In the Custom Setup dialog box, shown in Figure 4-23, select each of the listed options except VHD Mount, and select This Feature Will Not Be Available from the drop-down menu. After you have disabled all components except the VHD Mount tool, click Next.

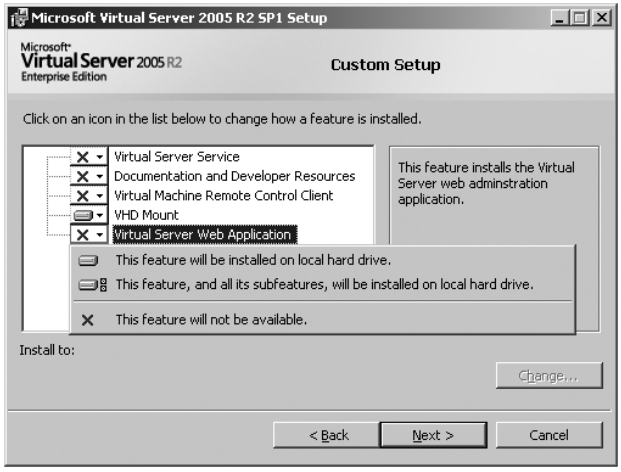

Figure 4-23 Enabling the VHD Mount tool

7. Click Install to complete the installation.

You should see the installation proceed, and then you will see an Internet Explorer window that provides a summary of the installation.

At this point, VHD Mount is installed into the C:\Program Files\Microsoft Virtual Server \VHDMount directory. A Start menu program group is not installed when you install VHD Mount because it is a command-line tool. To use VHD Mount, you must open a command prompt window and run the vhdmount.exe command with the correct command-line options to mount or unmount a .vhd file.

More Info For more information on VHDMount and the command-line options, refer to Chapter 5, "Advanced Features."

Uninstalling Virtual Server 2005 R2 SP1

Uninstalling Virtual Server 2005 R2 SP1 is a straightforward process. When you launch the uninstall process, the Virtual Server 2005 SP1 MSI file executes the predefined uninstall routine. This routine performs the following actions:

- Uninstalls the Virtual Server service
- Uninstalls the Virtual Machine Helper service
- Removes the Virtual Machine Monitor (VMM)
- Removes the Virtual Machine Network Services from all network interface cards that it is bound to
- Removes the Start menu Programs menu group and all shortcuts

If the Virtual Server Administration Website is installed on the local machine, the uninstall process also removes the IIS virtual directory, deletes the Administration Website files, removes any application pool configuration changes, and removes any files related to the Administration Website from the machine. The uninstall process does not remove IIS from the machine—that requires a separate uninstall step. Refer to Help and Support for your operating system version for instructions on how to uninstall IIS.

Any resource files that are stored locally on the machine or on a remote server will not be touched during the uninstall process. This means that you can uninstall Virtual Server 2005 R2 SP1 with no concern for loss of your virtual machines, virtual hard disks, or their configuration files. In addition, the Virtual Server configuration information file Options.xml is not removed from the system, so you can uninstall and reinstall Virtual Server without fear of losing your configuration settings.

The following procedures describe uninstalling Virtual Server 2005 R2 SP1. Instead of presenting one procedure for Windows XP and another procedure for Windows Server 2003 and Windows Vista, the various options are included in the appropriate steps. The Windows XP and Windows Server 2003 selections are presented first, followed by the Windows Vista selections.

To uninstall Virtual Server 2005 R2 SP1, complete the following steps:

1. Click the Start button, select Administrative Tools, and click Services.
2. Find the Virtual Server and the Virtual Machine Helper, right-click each one, and select Stop. This will stop both services and allow Virtual Server 2005 R2 SP1 to install. You cannot uninstall Virtual Server while the services are running.
3. Click the Start button, select Control Panel, click Add/Remove Programs or Uninstall A Program, depending on your operating system.

4. Find the entry for Virtual Server 2005 R2 SP1 in the list, and click either Remove or Uninstall, depending on your operating system. Figure 4-24 shows the dialog box for Windows XP and Windows Server 2003.

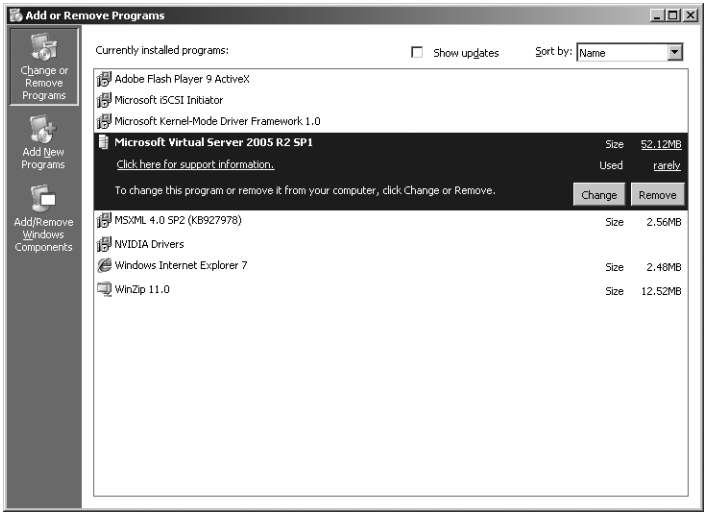

Figure 4-24 Uninstalling a program in Windows Server 2003 or Windows XP

5. Click Yes to confirm that you want to uninstall the Virtual Server 2005 R2 SP1 application and then click OK.

The uninstall process will launch, uninstall all components, and then finish.

Performing a Command-Line Installation

Microsoft Virtual Server 2005 R2 SP1 has a command-line installation interface that you can use to install or uninstall any combination of the installable Virtual Server components. The command-line interface is provided as part of the MSI file that is extracted from the Setup.exe provided by Microsoft. The command-line syntax contains a list of options that allow you to control the level of interface that is presented, from a full user interface to a quiet install with no visible interface. In addition, the command-line options allow you to control parameters such as the port used for the Administration Website and the state of the Virtual Server services.

This section presents the command-line options and explains how to use them to achieve the installation scenarios that were described in this chapter: single-server installation, central Administration Website, Virtual Server service, VMRC Client installation, Documentation and Developer Resources, and VHD Mount.

Command-Line Options

Performing a command-line installation of Virtual Server requires you to execute the command line from the local machine. To execute the command line with all available options, you must extract the Virtual Server 2005 Install.msi file from the Setup.exe file. Extracting the files requires the following syntax:

```
Setup.exe /c /t [drive letter:\path]
```

The meaning of each element in the syntax is as follows:

/c Extracts the contents of the Setup.exe file

/t Indicates the drive letter and path to use to extract the file will follow

drive letter:\path Specifies the drive letter and path in which to store the extracted files

For example, if you want to extract the Virtual Server 2005 Install.msi file to C:\VirtualServerSetupFiles, you would type the following on the command line and execute it.

```
Setup.exe /c /t c:\VirtualServerSetupFiles
```

Once you have extracted the Virtual Server 2005 Install.msi file, you need to understand the command-line options, the supporting parameters that are available to you, and how to use the .MSI file and Msiexec.exe file to achieve an installation from the command line. Table 4-4 lists the specific Msiexec.exe command-line options for Virtual Server 2005 Install.msi.

Table 4-4 Msiexec.exe Command-Line Options for Virtual Server 2005 Install.msi

Command-line option	Description
/i	Performs an installation of Virtual Server.
/a	Performs an administrative install of Virtual Server to a network location.
/x	Uninstalls an existing installation of Virtual Server.
/q[n,b,r,f]	Sets the user interface level based on the optional parameters specified. /q or /qn – No interface is provided (and no summary screen either) /qb – Basic user interface provided /qr – Reduced user interface provided /qf – Full user interface provided
/l {logfile}	Specifies where the setup log file is stored and the name of the log file. The *logfile* parameter must be specified as a full path, and environment variables can be used in the path. Examples: /l C:\logfiles\VirtualServerInstall.log /l %TEMP%\VirtualServerInstall.log

Table 4-4 Msiexec.exe Command-Line Options for Virtual Server 2005 Install.msi

Command-line option	Description
MSIFILE	Specifies the name of the MSI file that the Msiexec.exe file will launch. This must provide the full path to the MSI file or must be in the current directory.
ALLUSERS	Determines what users see in the Start menu and in Add Or Remove Programs. If ALLUSERS is not specified, a per-machine installation is performed (default). If ALLUSERS="" , the installer performs a per-user installation for the user that started the installation.
PIDKEY	Obsolete. This option is no longer needed. The PIDKEY is embedded in the installation MSI file and does not need to be specified.
SERVICESTARTUPMANUAL	Specifies whether the Virtual Server services (VSSRVC.EXE and VMH.EXE) are configured to start manually or automatically. 1 = Manual 0 = Automatic For example, to start the services manually: SERVICESTARTUPMANUAL=1
WEBSITEDEFAULTPORT	Specifies the default port that will be used for access to the Administration Website. If you do not specify a value, the default port number 1024 is used. Value = Port number For example: WEBSITEDEFAULTPORT=80
INSTALLDIR	Used in conjunction with the /i parameter to specify the custom directory path where you want Virtual Server to be installed. Not specifying this option will install Virtual Server to the default location C:\Program Files\Microsoft Virtual Server\. Value = the full path to the directory For example: INSTALLDIR=C:\VirtualServer
TARGETDIR	Used in conjunction with the /a parameter to specify the target directory in which you want Virtual Server administration installation to be placed. This option can be specified as a UNC path or a mapped driver letter and path. For example: TARGETDIR=\\SERVERA\Software\VirtualServer TARGETDIR=S:\VirtualServer

Table 4-4 Msiexec.exe Command-Line Options for Virtual Server 2005 Install.msi

Command-line option	Description
ADDLOCAL	Specifies the Virtual Server components that will be installed. One or more components can be specified, separated by commas. ADDLOCAL must be specified with all uppercase letters. **VirtualServer** – Virtual Server services **VMRCClient** – VMRC Client **DevAndDoc** –Documentation and Developer Resources **VSWebApp** – Administration Website **VHDMount** – VHD Mount tool For example, to install only the Administration Website, use the following: ADDLOCAL=VSWebApp To install the Virtual Server services, documentation and developer resources, and VHD Mount tool, use the following: ADDLOCAL=VirtualServer, DevAndDoc, VHDMount
NOSUMMARY	Specifies whether you want to display the summary screen at the end of the installation. Use a value of 1 to indicate the summary should not be displayed. The default is to display the summary. For example: NOSUMMARY=1

Command-Line Syntax

The MSIEXEC full command-line syntax is as follows:

```
msiexec.exe {/i|/a|/x} "msifile" [allusers=value] [servicestartupmanual=value]
[websitedefaultport=value] [{installdir=value|targetdir=value}] [ADDLOCAL=value,value]
[nosummary=value] [/qb | /qn | /qr | /qf] [/l logfile]
```

The following syntax line examples are for different scenarios (install on a local computer, administration installation, and uninstall) in which not all options are required.

Installing on a Local Computer

The following code block is a list of all the options and parameters that are available when performing an installation of Virtual Server 2005 R2 SP1 from the command line on a single server:

```
msiexec.exe /i "msifile" [allusers=value]
[servicestartupmanual=value] [websitedefaultport=value] [{installdir=value}]
[ADDLOCAL=value,value]
[nosummary=value] [/qb | /qn | /qr | /qf] [/l logfile]
```

Performing an Administrative Installation

The following code block is a list of all the options and parameters that are available when performing an administration installation of Virtual Server 2005 R2 SP1 on a remote server:

```
msiexec.exe /a "msifile" targetdir=value [/qb | /qn | /qr | /qf] [/l logfile]
```

Uninstalling an Existing Virtual Server Installation

The code block that follows is a list of all the options and parameters that are available when performing an uninstall of an existing installation of Virtual Server 2005 R2 SP1 on a local server:

```
msiexec.exe /x "msifile" [ADDLOCAL=value,value] [/qb | /qn | /qr | /qf] [/l logfile]
```

Important When you specify any path values in the command line and those paths contain spaces, you must enclose the entire path in quotes (" ").

Command-Line Examples

To perform a full installation of Virtual Server 2005 R2 SP1 on the local machine with no user interface and no logfile, use the following command line. This command line will use the default installation path, select the default Web administration port of 1024, and not provide a summary screen at the end of the installation.

```
msiexec.exe /I "virtual server 2005 install.msi" /qn
```

To change the default port that the Administration Website listens on from 1024 to port 80, you add the WEBSITEDEFAULTPORT=80 parameter to the command line:

```
msiexec.exe /I "virtual server 2005 install.msi" websitedefaultport=80 /qn
```

To perform an Administration install of Virtual Server 2005 R2 SP1 on a server named SERVER1, share named SOFTWARE, in a directory called VS2005R2SP1, with basic user interface (all on one line), use the following command line:

```
msiexec.exe /a "virtual server 2005 install.msi" targetdir=\\Server1\Software\VS2005R2SP1 /qb
```

To uninstall an existing Virtual Server installation with no user interface and a log file created and stored at C:\temp and called VS-UNINSTALL.LOG, use the following command line:

```
Msiexec.exe /X "Virtual Server 2005 Install.msi" /L C:\TEMP\VS-UNINSTALL.LOG /qn
```

Direct from the Source: Why Won't My Uninstall Command Line Work?

The Virtual Server uninstall process does not stop the Virtual Server and Virtual Machine Helper services prior to attempting to uninstall. You can use the NET STOP <*service name*> command for each service before launching an uninstall of the software. If you create a simple batch file with the following lines, uninstall will be successful:

```
Net Stop "Virtual Server"
Net Stop VMH
Msiexec /x "Virtual Server  2005 Install.msi" /qn
```

Mike Williams
Microsoft Services, Senior Consultant

Performing the Installation Scenarios Using the Command Line

This section describes how to use the command-line process to perform the same installation scenarios of Virtual Server 2005 R2 SP1: single-server installation, local Administration Website only, Virtual Server services only, Documentation and Developer Resources only, and VHD Mount tool only. You will specify that all of these command-line scenarios specify no user interface.

Single-Server Installation

```
Msiexec.exe /I "Virtual Server 2005 Install.msi" /qn
```

Local Administration Website Only

```
Msiexec.exe /I "Virtual Server 2005 Install.msi" ADDLOCAL=vswebapp /qn
```

Virtual Server Services Only

```
Msiexec.exe /I "Virtual Server 2005 Install.msi" ADDLOCAL=virtualserver /qn
```

Documentation and Developer Resources Only

```
Msiexec.exe /I "Virtual Server 2005 Install.msi" ADDLOCAL=devanddoc /qn
```

VMRC Client Tool Only

```
Msiexec.exe /I "Virtual Server 2005 Install.msi" ADDLOCAL=vmrcclient /qn
```

VHD Mount Tool Only

```
Msiexec.exe /I "Virtual Server 2005 Install.msi" ADDLOCAL=vhdmount /qn
```

Summary

In this chapter, we covered the installation and removal of Virtual Server 2005 R2 SP1, as well as how to upgrade an existing Virtual Server 2005 R2 installation. There are multiple possible installation scenarios based on operating system, desired Virtual Server components, and

component placement on servers. Determining which installation scenario applies to your environment and proactively collecting the required information will reduce installation issues. Distributing the Virtual Server 2005 R2 SP1 components across multiple servers will reduce the security risk of your environment, but that approach requires constrained delegation to be configured. The command-line installation process is the most flexible and easiest to use, and it should be your preferred method of installing or removing Virtual Server 2005 R2 SP1 in your environment.

Additional Resources

The following resources contain additional information and tools related to this chapter:

- Knowledge Base Article 890893, "The SPNs that Virtual Server requires are not registered in Active Directory when you try to install Virtual Server 2005 on a Windows-based domain controller," at *http://support.microsoft.com/kb/890893*
- Knowledge Base Article 322692, "How to raise domain and forest functional levels in Windows Server 2003," at *http://support.microsoft.com/kb/322692*
- Virtual Server 2005 R2 SP1 Administrator's Guide and Release notes available in the Microsoft Virtual Server menu option under the Start Menu
- Knowledge Base Article 314881, "The Command-Line Options for the Microsoft Windows Installer Tool Msiexec.exe," at *http://support.microsoft.com/kb/314881*
- IIS 6.0 Technical Reference in the Windows Server 2003 TechCenter, at *http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/69a58513-141a-4adb-b6bc-2aaad4ea77b8.mspx*

Chapter 5

Virtual Server 2005 R2 Advanced Features

In this chapter:

This chapter describes advanced features in Microsoft Virtual Server 2005 Release 2 (R2). You will learn about virtual hard disk, network, and clustering options that you can use to deploy broad virtualization infrastructure solutions. Technical descriptions and configurations are discussed along with common usage scenarios.

Using Virtual Hard Disk Advanced Features

Virtual Server 2005 R2 uses the virtual hard disk (VHD) format to encapsulate virtual machine data into one or more files that are equivalent to physical drives associated with a traditional server. Using the VHD format as a basic building block, Virtual Server 2005 R2 provides advanced virtual hard disk features that enable the creation of virtualized environments that are more functional and flexible than physical equivalents, particularly for disciplines such as development, testing, training, and support. Table 5-1 lists the advanced virtual hard disk features covered in this section.

Table 5-1 Virtual Hard Disk Advanced Features

Feature	Description
Differencing disks	A special type of dynamically expanding virtual hard disk that stores virtual machine data changes while isolating them from the base virtual hard disk.
Undo disks	A special type of dynamically expanding virtual hard disk that stores virtual machine data changes while isolating them from the base virtual hard disk. There are similarities with differencing disks, but differences in options and applicable scenarios.

Table 5-1 Virtual Hard Disk Advanced Features

Feature	Description
Linked disks	A special type of virtual hard disk designed specifically to convert a physical hard disk into a virtual hard disk file. The process associated with the use of linked disks is potentially time consuming depending on the size of the physical disk.
VHDMount command-line tool	This is a new feature provided with Virtual Server 2005 R2 SP1. VHDMount is an essential tool to manipulate virtual hard disk files without booting into a virtual machine.
VHD compaction	This tool is used to regain unused space within a virtual hard disk. The compaction process works only for dynamically expanding virtual hard disks. No other type of virtual hard disk can be compacted.

Differencing Disks

A virtual machine running within Virtual Server 2005 R2 has its data encapsulated in one or more base virtual hard disks. When data changes occur to the guest operating system or the applications running in it, modifications are committed to the virtual hard disks. The changes made to the virtual hard disks are permanent, paralleling the process that would occur with a standard physical system. However, a variety of compelling scenarios are enabled by preserving a base virtual hard disk in an unchanged state, while still capturing and storing ongoing virtual machine changes.

A differencing disk is a special type of dynamic disk that stores changes to virtual machine data in a separate file from a base virtual hard disk. The association of the base virtual hard disk to the differencing disk is defined as a parent-child relationship. In this parent-child relationship, each child differencing disk can derive from only one parent disk, but parent disks can be used as the basis to create multiple, distinct child differencing disks.

Figure 5-1 shows that differencing disks can be created in very simple or very complex parent-child hierarchies. A multilevel differencing disk hierarchy is commonly referred to as a *chain* of differencing disks, reflecting that a child differencing disk can have a parent disk that is also a differencing disk. The chain can consist of several levels, but it always stems from either a standard dynamically expanding or fixed-size virtual hard disk at the top of the hierarchy. This concept is important because data changes in a differencing disk are simply represented as modified blocks in relation to the parent disk. Therefore, a differencing disk is never used independently, but in conjunction with all parent disks in its hierarchy. (See Figure 5-1.)

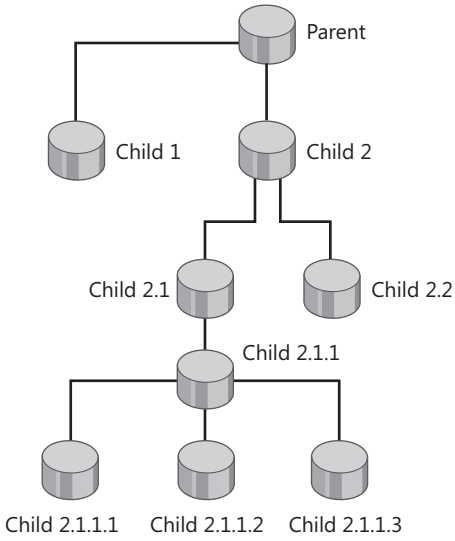

Figure 5-1 Multilevel differencing disk hierarchy

If you examine a Virtual Server 2005 R2 host file system, you will see each differencing disk stored as an individual file. Within the virtual machine file system, you see only a single disk, independent of how many levels of differencing disks are actually associated with a specific virtual hard disk.

Best Practices To quickly and easily identify parent-child differencing disk relationships in a complex chain, adopt a standardized virtual hard disk naming convention. The Virtual Server Administration Website allows you to inspect a differencing disk and discover its parent disk, but it does not report any child differencing disks related to it.

Creating a Differencing Disk

When you create a new differencing disk, the location of the base virtual hard disk that will be the parent for the new differencing disk must be specified. The parent disk can be either a fixed-size or dynamically expanding virtual hard disk. A differencing disk grows as needed, up to the size specified for the parent virtual hard disk.

To create a differencing disk, follow these steps:

1. Open the Virtual Server 2005 R2 Administration Website.
2. In the navigation pane, under Virtual Disks, point to Create and then click Differencing Virtual Hard Disk.
3. In Location, select the folder to store the new virtual hard disk file. If the folder does not appear in the list, type the fully qualified path to the folder as described in the next step.

4. In the Virtual Hard Disk File Name text box, type the fully qualified path to the folder followed by a name for the differencing virtual hard disk. You do not need to include a filename extension.
5. In Known Virtual Hard Disks, select the virtual hard disk file to use as the parent disk.
6. If the virtual hard disk file does not appear in the Known Virtual Hard Disks list, in the Fully Qualified Path To Parent Virtual Hard Disk text box, type the fully qualified path to the parent virtual hard disk file.
7. Click Create.

Note By default, differencing disks use the .vhd file extension, which makes them difficult to distinguish from standard virtual hard disks.

Examining Parent-Child Differencing Disk Relationships

Every dynamic disk contains a standard virtual hard disk header that embeds a specific dynamic disk header. The dynamic disk header format is identical for both standard dynamically expanding and differencing disks. However, several fields in this header are only relevant to differencing disks, as they identify parent disk attributes. A list of the dynamic disk header fields is provided in Table 5-2, with those relating only to differencing disks appearing in boldface type.

Table 5-2 Dynamic Disk Header

Dynamic disk header fields	Description
Cookie	A set field that identifies the header.
Data Offset	Absolute byte offset to next hard disk image structure (*currently unused*).
Table Offset	Absolute byte offset of the block allocation table (BAT) in the file.
Header Version	Dynamic disk header version.
Max Table Entries	Maximum number of entries in the BAT.
Block Size	Size of unit that is used to incrementally expand the dynamic disk.
Checksum	Checksum of the dynamic disk header.
Parent UUID	**128-bit universally unique identifier (UUID) of the parent disk (used only for differencing disks).**
Parent Time Stamp	**Modification time stamp of the parent disk (used only for differencing disks).**
Reserved	Field is set to zero.
Parent Unicode Name	**Unicode string for filename of the parent disk (used only for differencing disks).**

Table 5-2 Dynamic Disk Header

Dynamic disk header fields	Description
Parent Locator Entry 1	**Platform-specific format containing the absolute byte offset in the file where the parent locator is stored (used only for differencing disks).**
Parent Locator Entry 2	**Platform-specific format containing the absolute byte offset in the file where the parent locator is stored (used only for differencing disks).**
Parent Locator Entry 3	**Platform-specific format containing the absolute byte offset in the file where the parent locator is stored (used only for differencing disks).**
Parent Locator Entry 4	**Platform-specific format containing the absolute byte offset in the file where the parent locator is stored (used only for differencing disks).**
Parent Locator Entry 5	**Platform-specific format containing the absolute byte offset in the file where the parent locator is stored (used only for differencing disks).**
Parent Locator Entry 6	**Platform-specific format containing the absolute byte offset in the file where the parent locator is stored (used only for differencing disks).**
Parent Locator Entry 7	**Platform-specific format containing the absolute byte offset in the file where the parent locator is stored (used only for differencing disks).**
Parent Locator Entry 8	**Platform-specific format containing the absolute byte offset in the file where the parent locator is stored (used only for differencing disks).**
Reserved	Field is set to zero.

A differencing disk uses the parent UUID and Unicode file name information stored in its dynamic disk header to locate and open the parent disk. Because a parent disk can also be a differencing disk, it is possible that the entire hierarchy of parent disks will be opened, up to the base virtual hard disk.

Portability of parent and child differencing disks across server platforms is provided by the Parent Locator entries listed in Table 5-2. Parent locator entries store platform-specific information to locate the parent differencing disk on the physical drive.

Important For the Microsoft Windows platform, both the absolute (for example, c:\parent\parent.vhd) and relative (for example, .\parent\parent.vhd) paths of the parent disk are stored in the Parent Locator entry of a differencing disk. As long as you copy the virtual hard disks to the same relative directory hierarchy on a new host, you will be able to add the virtual machine to Virtual Server and turn it on without having to make any additional changes.

When a virtual machine using differencing disks issues a write operation, the data is written only to the child differencing disk. As part of the process, an internal virtual hard disk data structure is updated to reflect changes that supersede data in the parent disk. During read operations, the same internal virtual hard disk data structure is checked to determine which data to read from the child differencing disk. Unchanged data is read from the parent disk.

Direct from the Source: Configure Parent Disks as "Read-Only"

A child differencing disk stores the parent disk modification time stamp when it is created. Any modifications made to the parent disk after creation of the child differencing disk will be detected and will invalidate the child differencing disk. To ensure that nothing can be written to the parent disk that will corrupt the parent-child disk relationship, configure the parent disk as "read-only."

Bryon Surace
Program Manager, Windows Virtualization

Merging Differencing Disks

Although a differencing disk can be used to permanently store virtual machine data changes, you might need to combine the child differencing disk with the parent disk. Virtual Server 2005 R2 provides two ways to accomplish this. You can either merge the differencing disk into the parent disk or merge the differencing disk and the parent disk into a new virtual hard disk. If you merge a differencing disk into the parent disk, the differencing disk is deleted upon completion of the process and any other differencing disk that pointed to the original parent disk is invalidated. If you need to retain the differencing disk, you should choose to merge the differencing disk and parent disk into a new virtual hard disk. This approach is recommended to lower the risk of data loss. You can verify that the merge operation is successful prior to deleting the original files.

To merge differencing disks, follow these steps:

1. Open the Virtual Server R2 Administration Website.
2. In the navigation pane, under Virtual Disks, click Inspect.
3. In the Inspect Virtual Hard Disk pane, do one of the following, and then click Inspect:
   - ❑ In Known Virtual Hard Disks, select the virtual hard disk that you want to merge.
   - ❑ In the Fully Qualified Path To File text box, type the fully qualified path to the virtual hard disk file that you want to merge.
4. In the Actions pane, click Merge Virtual Hard Disk.
5. Proceed with one of the following two choices:
   - ❑ Select the Merge With Parent Virtual Hard Disk option.

- Select the Merge To New Virtual Hard Disk option, and then select a folder in which to store the new virtual hard disk. If the folder is not listed, type a fully qualified path and filename for the new virtual hard disk. You do not need to include a filename extension.

6. In Merged Virtual Hard Disk Type, select a type for the new virtual hard disk.
7. Click Merge.

Important Prior to merging a differencing disk and parent disk into a new virtual hard disk, make sure there is enough space on the physical disk to perform the operation.

Using Differencing Disks

Functionality gains from using differencing disks become evident when considering a typical support scenario. A support engineer often needs to troubleshoot server configurations for different operating system update levels or with different applications. Using one or more physical test servers, even with preconfigured build images, the setup and testing of multiple server configurations is a lengthy, complex process that results in protracted problem response time. Using Virtual Server 2005 R2 with differencing disks, a support engineer can quickly create a virtual machine for each unique server configuration. Starting with a common parent virtual hard disk that contains the base operating system, each individual server configuration is created as a new virtual machine with one or more differencing disks to capture incremental operating system patches and application stacks.

Important Differencing disks should not be used with cluster configurations.

As shown in Figure 5-2, implementing a virtualized support environment using differencing disks can help significantly reduce the setup and test cycle associated with problem resolution response time. Even with a single physical server constraint, a Virtual Server 2005 R2 host can run multiple virtual machines (VMs) concurrently, allowing parallel testing of distinctive server configurations. In addition to creating an environment that can lead to faster support response time, this solution also has the additional benefit of saving significant amounts of physical disk space for any scenario that requires multiple complex configurations sharing a large common software base.

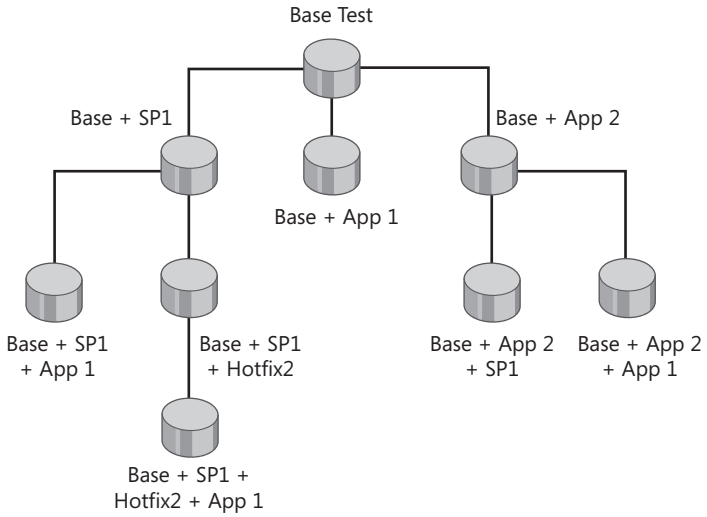

Figure 5-2 Using differencing disks to create guest VMs for concurrent testing

Undo Disks

Undo disks are quite similar to differencing disks. Like a differencing disk, an undo disk is used to isolate virtual machine data changes from a base virtual hard disk. Undo disks also share the special dynamic disk characteristics previously defined for differencing disks. However, in an environment where virtual machine data changes need to be quickly discarded or a rapid rollback to the base virtual machine state is required, undo disks are a better solution than differencing disks. There are other environments that require the use of a shared common software base and rapid rollbacks to a baseline state. In these cases, differencing disks can be used in combination with undo disks to implement the virtualization solution.

Note Unlike a differencing disk, which has a .vhd filename extension, an undo disk uses a .vud filename extension. Also, undo disks are stored in the same directory as the virtual machine configuration file (which uses a .vmc filename extension).

Configuring Undo Disks

One major distinction between differencing disks and undo disks is in the configuration process. A differencing disk is created at an individual virtual hard disk level and usually associated with the creation of a new virtual machine. In contrast, undo disks are either enabled or disabled for an existing virtual machine and created for every virtual hard disk associated with the virtual machine. In other words, you do not have the ability to individually choose the virtual hard disks for which undo disks are generated.

Important If you need to move a virtual machine from one Virtual Server 2005 R2 host to another, don't forget to move parent disks and virtual machine configuration files (.vmc) along with child differencing disks and undo disks.

To configure undo disks for a virtual machine, follow these steps:

1. Open the Virtual Server 2005 R2 Administration Website.
2. In the navigation pane, under Virtual Machines, point to Configure and then click the desired virtual machine.
3. In the Configuration section, select Hard Disks.
4. In the Virtual Hard Disk Properties section, select the Enable Undo Disks check box and then click OK.

Important Undo disks can be enabled or disabled only when a virtual machine is in a powered-off state. The option to enable undo disks is not available if the virtual machine is in a saved state.

Managing Undo Disks

Another major distinction between differencing disks and undo disks is that you are required to decide what to do with the changes saved in undo disks every time a virtual machine is shut down or placed in a saved state. Virtual Server 2005 R2 provides three options to manage undo disks:

- **Keep Undo Disks** This option saves the changes stored in the undo disk and preserves the state of the base virtual hard disk.
- **Commit Undo Disks** This option saves the changes stored in the undo disk to the base virtual hard disk.
- **Discard Undo Disks** This option deletes the undo disk without saving any changes to the base virtual hard disk.

If you shut down the guest operating system from within the virtual machine, undo disks are saved. If you choose to discard undo disk changes, new undo disks are created when the virtual machine is turned back on.

Caution If you disable undo disks while a virtual machine is turned off, the undo disks are immediately deleted.

Using Undo Disks

Undo disks are most useful in scenarios where frequent rollbacks to a base configuration are required. Two mainstream examples are software testing and end-user training. Working in these scenarios with only physical components, one of the most time consuming and tedious tasks is rebuilding the baseline environment—whether it is to re-create the steps to isolate a software bug or to prepare the system for the next user of a training lab. This is even more of a burden if the environment consists of several, incrementally different workloads, although the process can again be somewhat simplified by using imaging tools to more quickly reset each system. A better solution for working in these scenarios is to use Virtual Server 2005 R2 virtual machines that enable undo disks. As illustrated in Figure 5-3, the more complex software testing scenario—which requires multiple, incrementally different virtual machine configurations—is optimized by using undo disks in conjunction with differencing disks. The simple end-user training configuration only requires the implementation of undo disks. At the end of each training session, the system only needs to be reset to the base configuration.

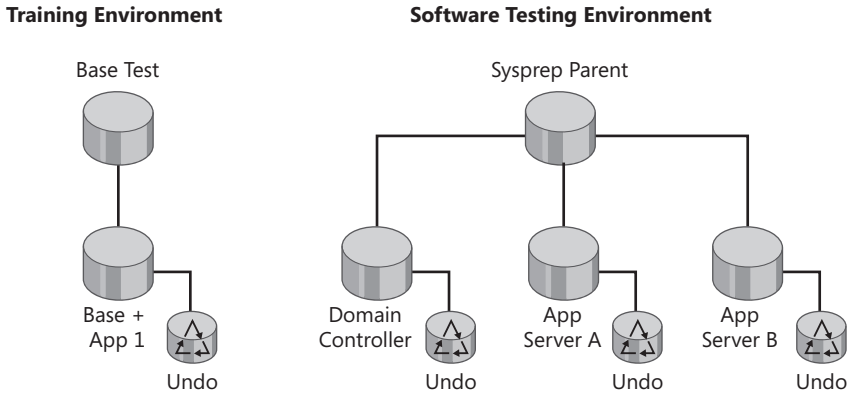

Figure 5-3 Using undo disks with and without differencing disks to achieve a quick rollback

In either case, a rollback to a baseline configuration is accomplished by simply choosing to discard the changes in the undo disks. This process takes just a few moments to complete before the system software is reset to the original configuration.

Best Practices To restrict the ability to commit undo disk changes and ensure the integrity of the virtual machine baseline configuration, you should set the base virtual hard disk files to read-only.

Linked Disks

A linked disk is a virtual hard disk that points to a physical drive with the single purpose of duplicating the contents into a new virtual hard disk. There are several requirements to con-

sider when using this method to migrate the contents of the physical disk into a virtual hard disk. The limitations are as follows:

- A linked disk can be associated only with a physical disk, not a volume.
- A linked disk must be used only to migrate a data disk; startup disks are not supported.
- A linked disk must be stored on a physical disk that is separate from the drive being converted.
- The physical disk must not be accessed by the host operating system or applications during the conversion process.
- If the physical disk that is being converted is larger than 127 GB, you must attach the virtual hard disk into which the disk contents will be copied to a virtual SCSI adapter.

Best Practices Prior to creating the linked disk, you should use the Disk Management Microsoft Management Console (MMC) or other similar tool to remove the drive letter for the target drive. This will make the drive inaccessible to the host operating system, preventing disk corruption during the conversion process.

Creating a Linked Disk

The creation of a linked disk is simple, but it is only the first step in converting a physical disk into a new virtual hard disk. Follow these steps to create a linked disk:

1. Open the Virtual Server 2005 R2 Administration Website.
2. In the navigation pane, under Virtual Disks, point to Create, and then click Linked Virtual Hard Disk.
3. In Location, select the folder in which to store the virtual hard disk file. If the folder you want does not appear in the list, you must type the fully qualified path to the folder in the following step.
4. In the Virtual Hard Disk File Name text box, after the path to the folder, type a name for the virtual hard disk. You do not need to include a filename extension.
5. In the Physical Computer Drive section, select the physical hard disk to which you want to link the virtual hard disk and then click Create.

At this point, you have only created a virtual hard disk that is essentially a pointer to the physical drive.

Using the Linked Disk to Convert the Physical Disk

To complete the process and copy the physical drive content to a new virtual hard disk, follow these additional steps:

1. Open the Virtual Server 2005 R2 Administration Website.
2. In the navigation pane, under Virtual Disks, click Inspect.
3. In the Inspect Virtual Hard Disk pane, select the virtual hard disk to convert in Known Virtual Hard Disks. If the file does not appear in the list, in the Fully Qualified Path To File text box, type the fully qualified path to the virtual hard disk file to convert.
4. Click Inspect.
5. Under Actions, click Convert Virtual Hard Disk.
6. In Location, select the folder in which to store the converted virtual hard disk file. If the folder you want does not appear in the list, in the Converted Virtual Hard Disk Name text box, type the fully qualified path including the filename.
7. In Converted Virtual Hard Disk Type, select the type of virtual hard disk that you want to create.
8. Click Convert.

Once the conversion process completes, you can attach the new virtual hard disk to a virtual machine. You should delete the linked disk that you created prior to the physical disk conversion.

Note Virtual Server 2005 R2 will prevent you from attaching a linked disk to a virtual machine.

VHDMount Command-Line Tool

The VHDMount command-line tool is a new feature delivered with Virtual Server 2005 R2 Service Pack 1 (SP1). This tool allows you to mount a virtual hard disk file as a virtual disk device on a host machine. Using this method, you can inspect, inject, or delete files in the virtual hard disk without having to boot into a virtual machine.

Note By default, the VHDMount command-line tool is located in %systemdrive%\Program Files\Microsoft Virtual Server\Vhdmount.

VHDMount leverages the Virtual Disk Service (VDS), which is a set of application programming interfaces (APIs) that permit management of disks and volumes at the operating system level. Although VDS is available only with Windows Server 2003 and later operating systems, you can still run VHDMount in Windows XP.

When VHDMount is used to mount a virtual hard disk file, VDS interacts with the Plug and Play Manager to discover the virtual hard disk as a new disk and mount it (assigning a drive letter) in the host operating system. Once the virtual hard disk is successfully mounted, a new entry is listed in Device Manager | Disk Drives and is registered as *MS Virtual Server SCSI Disk*

Device. There is also a new entry listed in Device Manager | Microsoft Server Virtual Storage Devices that is registered as *Microsoft Server Virtual Storage DeviceXX*, where *XX* is a unique number that increases sequentially with each mounted device. At this stage, the virtual hard disk file contents can be accessed using standard file system browsing tools such as Windows Explorer.

Important By default, all changes made by VHDMount to a mounted disk are written to an undo disk that is created in the temporary folder for the current user. You can use the /f option to mount a VHD without an undo disk. You can also use the /c option to commit or /d option to discard changes when unplugging a mounted disk.

Defining VHDMount Command-Line Options

VHDMount is a simple utility to use, with only a few options needed to mount and dismount virtual hard disks. Table 5-3 lists the VHDMount command-line options.

Table 5-3 VHDMount Command-Line Options

Command-line option	Description
/p	Plugs in a virtual hard disk file as a virtual disk device without mounting the volume.
/m	Plugs in a virtual hard disk file as a virtual disk device and mounts the volume.
/u	Unplugs a virtual disk device.
/q	Returns the disk name of a mounted virtual disk device.

Important Even though VDS is not available in Windows XP, the virtual disk device should be automatically detected and mounted. However, because you cannot use the /m option with VHDMount, you are unable to specify a starting drive letter to mount a virtual hard disk in Windows XP.

Using VHDMount to Plug In a Virtual Hard Disk File

The following command-line shows the VHDMount option and parameter needed to plug in a virtual hard disk file without mounting the volume:

```
VHDMOUNT.EXE /p [/f] VHDFileName
```

VHDFileName VHDFileName indicates the fully qualified path to the virtual hard disk file. If you use the /f option, an undo disk will not be created. For example, to plug in a virtual hard disk file named test.vhd (with an undo disk) located in folder c:\virtual machines, you type the following:

```
VHDMOUNT.EXE /p "c:\virtual machines\test.vhd"
```

Important When you specify any path values in the command line and those paths contain spaces, you must enclose the entire path in quotes.

Using VHDMount to Plug In and Mount a Virtual Hard Disk File

The next command line shows the VHDMount option and parameter needed to plug in and mount a virtual hard disk file:

```
VHDMOUNT.EXE /m [/f] VHDFileName [DriveLetter]
```

DriveLetter is an optional parameter that defines the starting drive letter used to mount virtual hard disk files.

For example, to plug in and mount the virtual hard disk file used in the previous example as drive E, you type the following:

```
VHDMOUNT.EXE /m "c:\virtual machines\test.vhd" E
```

Important When you specify a drive letter in your VHDMount command, do not type a colon after the drive letter. If you do, the VHDMount help screen will display and your command will be ignored.

Using VHDMount to Unmount a Virtual Hard Disk File

The following command line represents the VHDMount option and parameters needed to unmount a virtual hard disk file:

```
VHDMOUNT.EXE /u [/c | /d] VHDFileName | All
```

All is an optional parameter that applies the operation to all mounted virtual disk devices. The /c option updates the original VHD with all the changes stored in the undo disk (if one was created) and deletes the undo disk after unplugging the disk. The /d option discards all changes to the mounted disk and deletes the undo disk after unplugging the disk. The /c and /d options are only applicable if the VHDMount /p and /m commands were used without the /f option.

For example, to dismount a virtual hard disk file, update the original VHD, and delete the undo disk, you type the following:

```
VHDMOUNT.EXE /u /c "c:\virtual machines\test.vhd"
```

Using VHDMount to Determine a Virtual Hard Disk Name

The next command line shows the VHDMount option and parameter needed to determine the disk name associated with the mounted virtual hard disk file:

```
VHDMOUNT.EXE /q VHDFileName | All
```

All is an optional parameter that applies the operation to all mounted virtual disk devices.

For example, to get a listing of disk names associated with all mounted virtual hard disk files, you type the following:

```
VHDMOUNT.EXE /q All
```

On the Companion Media On the companion media, you will find a directory called \Chapter Materials\Files\VHDMount. Inside the directory there is a registry file named Vhdmenu.reg. This file will make registry modifications that add mount and dismount selections to the context menu that appears when you right-click a virtual hard disk file.

VHD Compaction

VHD compaction is a process that reduces the size of a virtual hard disk file on the physical disk. Virtual Server 2005 R2 provides a compaction tool that achieves minor reductions in a virtual hard disk file size if used solely on its own. A better approach is to use a three-step process that includes defragmentation, precompaction, and compaction. Defragmentation and precompaction prepare the virtual hard disk file for the compaction process, resulting in greater reductions in virtual hard disk file size.

Note Prior to virtual hard disk file defragmentation, remove temporary files and folders, delete any other unwanted data, and empty the recycle bin.

VHD compaction can be performed only on dynamically expanding disks. Fixed-size virtual hard disks have to be converted to a dynamically expanding disk prior to being compacted. Special dynamically expanding virtual hard disks, such as differencing or undo disks, cannot be directly compacted. Differencing disks and undo disk changes must be merged into their parent disk, and the parent disk can be compacted if it is a dynamically expanding disk.

Best Practices Because of processor and disk resource requirements, you should use a non-production server, when possible, to perform the virtual hard disk compaction process. In Virtual Server 2005 R2, you can perform the defragmentation step within the virtual machine or while the virtual hard disk is offline. However, it is best to perform defragmentation, precompaction, and compaction with the virtual hard disk file offline.

Defragmenting the Virtual Hard Disk File

The first step in the process to reduce the size of a virtual hard disk file is defragmentation. As new information is written to disk, data might not be saved in contiguous disk blocks. In time, as you delete data on the disk, empty blocks will be randomly filled with file fragments. Performance is adversely affected when the disk fragmentation is excessive because it takes longer to retrieve related data spread across a disk than if it were located in a contiguous set of blocks. Defragmentation reduces or eliminates the number of fragmented files on a disk, resulting in larger areas of empty contiguous blocks.

To defragment a virtual hard disk offline, you first have to use the VHDMount command-line tool to mount the virtual hard disk file. You can find the VHDMount command syntax in the

"Using VHDMount to Plug In and Mount a Virtual Hard Disk File" section earlier in this chapter. Once the virtual hard disk file is mounted, use the Windows Defrag utility on the host system to defragment the virtual hard disk file. Table 5-4 lists the defrag command lines for Windows XP, Windows Server 2003, and Windows Vista. The time required to defragment the virtual hard disk file depends on several factors, including the degree of fragmentation, file size, and disk characteristics.

Table 5-4 Platform-Specific Defragmentation Command Lines

Command line	Operating system
Defrag *DriveLetter* ■ *DriveLetter* is the drive letter associated with the mounted virtual hard disk.	Windows XP Windows Server 2003
Defrag *DriveLetter* –w ■ *DriveLetter* is the drive letter associated with the mounted virtual hard disk. ■ –*w* specifies that all file fragments should be consolidated, regardless of size.	Windows Vista

Precompacting the Virtual Hard Disk File

The second step in the process is precompaction. Virtual Server 2005 R2 includes the Virtual Disk Precompactor tool, which is designed to overwrite any unallocated disk blocks in a virtual hard disk file with zeros. This step is crucial to ensure that the compaction tool can make the virtual hard disk file as small as possible.

The Virtual Disk Precompactor tool is contained in the Precompact.iso disk image located in the %systemdrive%\Program Files\Microsoft Virtual Server\Virtual Machine Additions folder. Use your favorite virtual CD tool to mount the Precompact.iso image on your Virtual Server 2005 R2 host and retrieve the Precompact.exe tool. Table 5-5 lists the options that are available when you invoke the Virtual Disk Precompactor tool from the command line.

Table 5-5 Virtual Disk Precompactor Command-Line Options

Command-line option	Description
-Help	Displays the help dialog box that lists the command-line options, product version, and syntax examples.
-Version	Displays the help dialog box that lists the command-line options, product version, and syntax examples.
-Silent	Executes the precompactor in unattended mode, and suppresses all dialog boxes.

Table 5-5 Virtual Disk Precompactor Command-Line Options

Command-line option	Description
-SetDisks:<list> <*list*> is an optional parameter that represents one or more drive letters.	Defines the list of virtual hard disks to precompact. If this option is not specified, all virtual hard disks attached to a virtual machine are compacted.

For example, the following command precompacts virtual hard disks mounted to drive letters F and G, in unattended mode:

```
Precompact –Silent –SetDisks:FG
```

More Info Virtual Server 2005 R2 allows precompacting virtual hard disk files from within a virtual machine. Once you capture the Precompact.iso image on the virtual machine CD or DVD drive, you can double-click the drive to launch Virtual Disk Precompactor. Using this process, you cannot specify which virtual hard disk to precompact. Instead, Virtual Disk Precompactor precompacts all virtual hard disks attached to the virtual machine.

Compacting the Virtual Hard Disk File

The third and final step in the process to reduce the virtual hard disk size is disk compaction. After running the Virtual Disk Precompactor tool, empty disk blocks in the virtual hard disk file contain zeros. The Virtual Server compaction tool finds the disk blocks that contain zeros and removes them, reducing the virtual hard disk file size.

Caution The Virtual Server compaction tool requires that you have enough disk space to concurrently store the original virtual hard disk file and an additional temporary file that contains the compacted virtual hard disk. The original virtual hard disk file will be deleted at the end of the compaction process and replaced with the compacted virtual hard disk file. If the disk runs out of space before completing the compaction process, an event will be recorded in the Virtual Server event log and no changes will be made to the disk.

To use the Virtual Server compaction tool, follow these steps:

1. Open the Virtual Server 2005 R2 Administration Website.
2. Turn off the virtual machine associated with the dynamically expanding virtual hard disk that you want to compact.
3. In the navigation pane, under Virtual Disks, click Inspect.
4. In the Inspect Virtual Hard Disk pane, select the virtual hard disk to compact in Known Virtual Hard Disks. If the virtual hard disk file does not appear in the list, type the fully qualified path to the virtual hard disk in the Fully Qualified Path To File text box.

5. Click Inspect.
6. Under Actions, click Compact Virtual Hard Disk.
7. In the Compact Virtual Hard Disk pane, click Compact.

The VHD compaction process can also be scripted using the Virtual Server 2005 R2 COM API. This API allows you to create scripts and compact the virtual hard disk files outside of the Virtual Server Administration Website.

On the Companion Media On the companion media, you will find a directory called \Chapter Materials\Scripts\Compact. Inside the directory there are two files, Vhdprep.bat and Compaction.vbs. The Vhdprep.bat file mounts the virtual hard disk file and runs the defragmenter and Virtual Disk Precompactor before calling the Compaction.vbs script. The Compaction.vbs script invokes the Virtual Server compaction tool to compact the virtual hard disk offline.

Using Virtual Network Advanced Features

The Virtual Server 2005 R2 network architecture allows virtual machine network traffic to be isolated from other virtual machines, the Virtual Server 2005 R2 host, and external networks. It also allows virtual machines to be connected to each other, the Virtual Server 2005 R2 host, corporate networks, and the Internet. Many configuration options are available and some depend on the implementation of advanced network settings. Table 5-6 lists Virtual Server 2005 R2 advanced network features covered in this section.

Table 5-6 Virtual Network Advanced Features

Configuration	Description
Microsoft Loopback Adapter	A software-based network adapter that is used to connect virtual machines to internal networks.
Host-to-Guest Networking	Uses the Microsoft Loopback Adapter to enable network connectivity between a Virtual Server 2005 R2 host and virtual machines.
Internet Connection Sharing with Network Address Translation	Uses the Microsoft Loopback Adapter to enable virtual machines to share the Virtual Server 2005 R2 server network access to the Internet.

Using the Microsoft Loopback Adapter

The Microsoft Loopback Adapter is a built-in, software-based network interface that can be attached to virtual networks to provide connectivity between virtual machines. The Microsoft Loopback Adapter can also be used to attach to internal virtual networks linking virtual machines to the Virtual Server 2005 R2 host. Network traffic between virtual machines and the Virtual Server 2005 R2 host is constrained to the internal virtual networks and isolated from external, physical networks.

Installing the Microsoft Loopback Adaptor

The Microsoft Loopback Adaptor is installed on the Virtual Server 2005 R2 host just like a physical network adapter. Here are the steps to install the Microsoft Loopback Adaptor on Windows Server 2003 R2:

1. On the Virtual Server 2005 R2 host, click Start and then click Control Panel.
2. In Control Panel, click Add Hardware and then click Next.
3. In the Is The Hardware Connected dialog box, choose Yes (I Have Already Connected The Hardware) and then click Next.
4. In the Installed Hardware list, choose Add A New Hardware Device and then click Next.
5. In the What Do You Want The Wizard To Do check list, choose Install The Hardware That I Manually Select From A List (Advanced) and then click Next.
6. In the Common Hardware Types list, choose Network Adapters and then click Next.
7. In the Manufacturer list, click Microsoft.
8. In the Network Adapter list, choose Microsoft Loopback Adapter and then click Next.
9. In the Hardware To Install dialog box, click Next.
10. In the Completing The Add Hardware Wizard dialog box, click Finish.

Important You must be a member of the administrators group to install a new network adapter in the Virtual Server host operating system.

Configuring the Microsoft Loopback Adaptor

Before you can use the Microsoft Loopback Adaptor, you must ensure that it is properly configured on your Virtual Server 2005 R2 host. The Microsoft Loopback Adaptor must be bound to Virtual Machine Network Services to allow communications through a virtual network. Once the configuration is complete, you can create virtual networks in the Virtual Server 2005 R2 Administration Website to enable virtual machine network connectivity. Follow these steps to configure the Microsoft Loopback Adaptor bindings on the Virtual Server 2005 R2 host:

1. On the Virtual Server 2005 R2 host, click Start and select Control Panel.
2. Select Network Connections, right-click the local area connection associated with the Microsoft Loopback Adapter and then click Properties.
3. In This Connection Uses The Following Items, ensure that the Virtual Machine Network Services check box is selected.
4. Click Internet Protocol (TCP/IP), and then click Properties.

5. On the General tab, select Use The Following IP Address and then type the IP address and subnet mask, but do not enter a gateway address.
6. Click OK, and then click Close.

Note Use one of the reserved ranges of nonroutable TCP/IP addresses when you configure the Microsoft Loopback Adaptor network address properties. The network address and network mask must be the same on the Virtual Server 2005 R2 host as on the virtual machines that you want to connect to the virtual network.

Implementing Host-to-Guest Networking

Virtual PC 2007 has a Shared Folders feature that allows file sharing between the Virtual PC host and virtual machines. Although no similar feature exists in Virtual Server 2005 R2, you can use the Microsoft Loopback Adapter and virtual networks to enable network connectivity between a Virtual Server 2005 R2 host and virtual machines. Once you have configured this arrangement, you can use standard Windows file sharing features between the physical server and virtual machines.

Creating a Virtual Network for Host-to-Guest Networking

After the Microsoft Loopback Adapter has been installed and configured on the Virtual Server 2005 R2 host, you can create a new virtual network to which you connect the virtual machines. To accomplish this, perform the following steps:

1. Open the Virtual Server 2005 R2 Administration Website.
2. In the navigation pane, under Virtual Networks, click Create.
3. In the Virtual Network Name text box, type a name for the virtual network.
4. In Network Adapter On Physical Computer, select the Microsoft Loopback Adapter.
5. In Disconnected Virtual Network Adapters, select the Connected check box for any virtual machine network adapter that you want to attach to the new virtual network.
6. In the Virtual Network Notes text box, type in a description for the new virtual network and then click OK.

You can now boot the virtual machines, configure the network address for the new local connection, and configure firewall settings to enable resource sharing, as required.

Enabling a Virtual DHCP Server on a Virtual Network

If you intend to connect several virtual machines to the host-to-guest virtual network, you should configure the Virtual DHCP Server option on the virtual network. The Virtual DHCP

server will manage and provide network configuration options to connecting virtual machines. These are the steps to enable the Virtual DHCP Server option:

1. Open the Virtual Server 2005 R2 Administration Website.
2. In the navigation pane, under Virtual Networks, select Configure and then click the appropriate virtual network.
3. In the Virtual Network Properties pane, click DHCP server.
4. Choose the Enabled check box, and configure the DHCP server options as needed.
5. Click OK.

Note In the DHCP Server options, you can see that the first 16 IP addresses from the start of the specified range are reserved. These 16 IP addresses are never assigned; use one in that range to configure the Virtual Server host adapter.

Configuring Internet Connection Sharing and Network Address Translation

Using the Microsoft Loopback Adapter, you can also configure Internet Connection Sharing (ICS) on the Virtual Server 2005 R2 host to provide virtual machine connectivity to external networks using Network Address Translation (NAT). This configuration provides external network access without the provisioning of official network addresses or direct virtual machine connection to the physical network. The major steps to implement this scenario are as follows:

1. Install the Microsoft Loopback Adapter on the Virtual Server 2005 R2 host.
2. Configure Internet Connection Sharing on the Microsoft Loopback Adapter.
3. Create a virtual network using the Microsoft Loopback Adapter.
4. Connect virtual machines to the virtual network.

All steps are covered in previous examples, with the exception of the Internet Connection Sharing configuration on the Virtual Server 2005 R2 host. Here are the steps to complete the Internet Connection Sharing configuration on Windows Server 2003 R2:

1. On the Virtual Server 2005 R2 host, click Start and select Control Panel.
2. Select Network Connections, and click on the connection that provides Internet connectivity.
3. In the Local Area Connection Status dialog box, on the General tab, click Properties.
4. Click the Advanced tab.

5. In Internet Connection Sharing, select the Allow Other Network Users To Connect Through This Computer's Internet Connection check box.
6. Click OK.

You can use the network connection Repair option in the virtual machines to force connections to refresh the IP address configuration from the Internet Connection Sharing host.

Caution If IPSec is configured on the Virtual Server 2005 R2 host, you cannot use Internet Connection Sharing to provide external network access to virtual machines.

Using Clustering Advanced Features

A common issue that arises when considering the deployment of a virtualized infrastructure is that a single physical server running multiple workloads becomes a more critical point of failure, with an impact on a larger user and business base than a single physical server running a single workload. Clustering addresses this risk by providing high-availability solutions that are as applicable in the virtualization space as in the physical server space. In this section, you will learn how to configure virtual machines and Virtual Server 2005 R2 hosts to implement the clustering scenarios listed in Table 5-7.

Table 5-7 Virtual Server 2005 R2 Advanced Cluster Configurations

Feature	Description
Virtual Machine Cluster Using iSCSI	A cluster based on Microsoft Cluster Server (MSCS) that consists of two or more virtual machine cluster nodes supporting a cluster-aware application. Virtual machine cluster nodes can be located across Virtual Server 2005 R2 hosts, but they require iSCSI-based disks.
Virtual Server Host Cluster	A cluster based on Microsoft Cluster Server that consists of two or more Virtual Server 2005 R2 host cluster nodes.

In Virtual Server 2005, you could create only a two-node virtual machine cluster based on virtual SCSI adapters. This required the cluster nodes to be located on the same Virtual Server 2005 host. A two-node virtual machine cluster could be useful in test environments using cluster-aware applications, but it was not a solution that could be deployed and supported in a production environment. In effect, the Virtual Server 2005 host represented a single point of failure, so the solution could not meet high-availability production requirements.

Virtual Server 2005 R2 removed the two-node and single-host virtual machine cluster limitations by adding support for the iSCSI protocol. Using iSCSI shared disks, multinode clusters can be created using virtual machines hosted on separate Virtual Server 2005 R2 hosts. This type of cluster is still recommended for virtual machines running cluster-aware applications.

Virtual Server 2005 R2 also introduced support for Virtual Server host clusters. Virtual Server 2005 R2 host clusters allow failing over individual or all virtual machine workloads to other Virtual Server 2005 R2 host cluster member nodes. For virtual machines running non–cluster aware applications, Virtual Server 2005 R2 host clusters are a basic building block for the implementation of high-availability solutions.

Virtual Server 2005 R2 SP1 includes all the clustering features found in Virtual Server 2005 R2. Once you have installed Virtual Server 2005 R2 SP1 on a host, you will have access to a whitepaper with detailed information concerning Virtual Server 2005 R2 host clusters. Previously provided as a download from the Microsoft Web site, the whitepaper is now packaged in the Virtual Server 2005 R2 SP1 distribution media. You can find the whitepaper in the %systemdrive%\Program Files\Microsoft Virtual Server\Host Clustering directory on your Virtual Server 2005 R2 SP1 host.

Implementing a Virtual Machine Cluster Using iSCSI

With Virtual Server 2005 R2 SP1, virtual machine clusters are now supported for production workloads when used in conjunction with iSCSI-based shared disk systems. Using iSCSI to deploy a cluster eliminates the need for the specialized hardware that was previously required to configure clustering. The requirements for an iSCSI-based solution are network adapters to connect the storage to the cluster nodes, and a storage unit that uses iSCSI. The iSCSI protocol defines the rules and processes for transmitting and receiving block storage data over TCP/IP networks. iSCSI-based implementations consist of an iSCSI initiator and an iSCSI target with an interconnecting network.

Virtual machine clusters implemented with iSCSI require each cluster node to be located on separate Virtual Server 2005 R2 hosts. Virtual machine clusters can range from two-node to eight-node active clusters. Physical distance between cluster nodes is restricted by the iSCSI protocol and the maximum latency that a cluster heartbeat signal can support.

Table 5-8 lists implementation requirements prior to creating a two-node virtual machine cluster based on an iSCSI storage device.

Table 5-8 Requirements for an ISCSI-Based Virtual Machine Cluster

Requirement	Description
Operating System	Windows Server 2003 R2 Enterprise Edition must be installed on each virtual machine cluster node.
Virtual Machine Additions	Virtual Machine Additions must be installed on each virtual machine node.
iSCSI Quorum and Shared Disks	iSCSI Quorum and Shared Disks targets must be created prior to configuring the cluster nodes. The Quorum disk must be at least 50 MB in size to satisfy Microsoft Cluster Server requirements.

Table 5-8 Requirements for an ISCSI-Based Virtual Machine Cluster

Requirement	Description
Network Adapters	Three network adapters must be added and configured for the Public, Private, and iSCSI networks on each virtual machine cluster node.
Virtual Networks	Virtual networks must be created for non-cluster traffic and iSCSI traffic (Public, Private, and iSCSI).
Active Directory	Virtual machine cluster nodes must be members of an Active Directory domain.
Cluster Service Account	A cluster service account must be created in Active Directory.

To deploy a two-node virtual machine cluster using iSCSI, you must perform the following major steps:

1. Create a shared drive for quorum and data storage using the iSCSI Initiator.
2. Configure virtual networks on each of the Virtual Server 2005 R2 hosts.
3. Configure shared drives on each virtual machine cluster node.
4. Install Microsoft Cluster Server on the first virtual machine cluster node and assign the shared drive.
5. Install Microsoft Cluster Server on the second virtual machine cluster node, join it to the cluster, and assign the shared drive.

Note The Microsoft iSCSI Initiator service is included in the Microsoft iSCSI Software Initiator package, which you can download from the Microsoft Web site at *http://go.microsoft.com/fwlink/?linkid=44352*.

Configuring the iSCSI Shared Disks

After you build your base virtual machines, you can configure the cluster shared disks. Follow these steps to configure virtual machine cluster node access to iSCSI shared disks:

1. Install the Microsoft iSCSI Initiator software in the first virtual machine.
2. Click Start, click All Programs, click Microsoft iSCSI Initiator, and then click Microsoft iSCSI Initiator again.
3. Click the Discovery tab, and in Target Portals, click Add.
4. Enter the name or IP address of the server where the target iSCSI drive is defined.
5. Click the Targets tab to display a list of disk targets.
6. Select Quorum and click Log On.

7. Select Automatically Restore This Connection When The System Boots And Enable Multipath, if you have multipath software installed.
8. Repeat steps 6 and 7 for the Shared target, and then click OK.
9. In the Disk Management MMC, format each disk with a single partition, using drive letter Q for the Quorum disk and drive letter S for the Shared disk.
10. Shut down the virtual machine.
11. Repeat steps 1 to 8 for the second virtual machine.
12. In the Disk Management MMC, set the Quorum drive letter to Q and the Shared drive letter to S.

Configuring Microsoft Cluster Server on the First Virtual Machine

When you create the first node in a cluster, you specify all parameters that define the cluster configuration. The Cluster Configuration Wizard guides you through the installation and completes the cluster setup when you have entered all the required information.

Caution During the configuration of Microsoft Cluster Server on the first cluster node, you must power-off all other nodes. This is to avoid data corruption on the shared disks. Ensure that the first cluster node can successfully access all volumes before attempting to join additional cluster nodes.

Follow these steps to configure Microsoft Cluster Server on the first virtual machine cluster node:

1. Log in to the virtual machine with Domain Administrator credentials.
2. Click Start, click All Programs, click Administrative Tools, and then click Cluster Administrator.
3. When prompted with the Open Connection To Cluster dialog box, select Create New Cluster in the Action drop-down list.
4. Review the information list in the New Server Cluster Wizard, and then click Next.
5. In the Cluster Name text box, type a name for the cluster and then click Next.
6. In the Computer Name text box, type the computer name of the virtual machine that is the first node in the cluster.
7. Click Next.
8. Remedy any errors found in the Analyzing Configuration step, and then re-analyze. If there are no further errors, click Next.
9. In the IP Address text box, type an IP address on the public network that will be used to manage the cluster and click Next.

10. In the User Name text box, type the name of the cluster service account that you created in Active Directory.
11. In the Password text box, type the password for the cluster service account.
12. In Domain, select your domain name from the drop-down list and then click Next.
13. Review the Summary page to verify that all information used to create the cluster is correct.
14. Click Quorum, select Disk Q: from the drop-down list, and then click OK.
15. Click Next.
16. Once the cluster creation is complete, click Next.
17. Click Finish to complete the installation.

Configuring Microsoft Cluster Server on the Second Virtual Machine

Installing Microsoft Cluster Server on the second virtual machine is much quicker because the cluster configuration already exists. Additional cluster nodes are simply joined to the defined cluster.

When adding subsequent nodes, leave the first cluster node and all shared disks turned on, and power-up additional nodes. The cluster service will control access to the shared disks to eliminate any chance of corruption. Follow these steps to configure the second node (and any subsequent node) in the cluster:

1. Open Cluster Administrator on the first cluster node.
2. Click File, click New, and then click Node.
3. On the Add Cluster Computers Wizard Welcome page, click Next.
4. In the Computer Name text box, type the computer name for the second cluster node and then click Add.
5. Click Next.
6. Remedy any errors found in the Analyzing Configuration step, and then re-analyze. If there are no further errors, click Next.
7. Type the password for the cluster service account, and then click Next.
8. Review the summary information that is displayed for accuracy, and then click Next.
9. Review any warnings or errors encountered during cluster creation, and then click Next.
10. Click Finish to complete the installation.

To quickly verify that cluster failover is successful, you can shut down the first cluster node. When you open Cluster Administrator on the second cluster node, you will see that it now

owns all cluster resources. Once you have tested that cluster failover is successful, you can proceed with the installation of the cluster-aware application.

Implementing a Virtual Server Host Cluster Using iSCSI

To achieve high availability for non–cluster aware applications running in virtual machines, you must implement a Virtual Server 2005 R2 host cluster. Virtual Server 2005 R2 host clusters can be deployed using SCSI, SAN, or iSCSI-based shared storage. Like virtual machine clusters, Virtual Server 2005 R2 host clusters can range from two-node to eight-node active clusters. It is important to understand that in this configuration, you are clustering the Virtual Server 2005 R2 hosts, not the applications running in the virtual machines. If one of the Virtual Server 2005 R2 host cluster nodes fails, virtual machines defined as resource groups in the cluster configuration are restarted on other Virtual Server 2005 R2 host cluster member nodes. In contrast, failure of an application running within a virtual machine will not result in a failover event.

Important The complete set of hardware used to implement a Virtual Server Host cluster must be listed in the Windows Server Catalog as a qualified cluster solution for Windows Server 2003.

There are many scenarios to which you can apply a Virtual Server 2005 R2 host cluster solution. Table 5-9 lists the most common scenarios that benefit from a Virtual Server 2005 R2 host cluster implementation.

Table 5-9 Virtual Server Host Cluster Scenarios

Scenario	Virtual Server host cluster benefits
Host hardware scheduled maintenance	Prior to performing hardware maintenance on a Virtual Server cluster node, hosted virtual machines can move groups over to other nodes in the cluster with minimal impact on application availability.
Host software updates	Before applying potentially disruptive software updates to the host, hosted virtual machines can fail over to other nodes in the cluster with minimal impact on application availability.
Non–cluster aware applications	Non–cluster aware applications running in virtual machines on a Virtual Server 2005 R2 host cluster node are protected from unexpected downtime caused by a host failure. If the Virtual Server 2005 R2 host cluster node fails, the virtual machine can fail over to other nodes in the cluster with minimal impact on application availability.

Table 5-9 Virtual Server Host Cluster Scenarios

Scenario	Virtual Server host cluster benefits
Workload rebalancing	Virtual machine performance might dictate a need to rebalance the workload on a Virtual Server 2005 R2 host cluster node. If there is another cluster node with the required resources available, the virtual machine can be quickly failed over with minimal impact on application availability.

During an unplanned cluster failover event, there is always some short period of time during which the cluster-defined resources are unavailable as they are restarted on a different cluster node. Microsoft Cluster Server ensures that the applications experience minimal service disruptions. If an administrator performs a normal shutdown on a cluster node or moves a guest from one host to another for planned maintenance, Virtual Server 2005 R2 can save the virtual machine state before it is moved.

Because virtual machines running in Virtual Server 2005 R2 are not cluster-aware, Microsoft created a script that ensures that virtual machines function correctly during cluster failover events. Each virtual machine is configured as a cluster resource group. Inside each cluster resource group, the script is configured as a Generic Script resource that has the effect of turning a virtual machine into a cluster-aware-like application. The script can also restart a virtual machine when it stops running. Underlying this whole process is the Microsoft Cluster Server, which provides the health monitoring and automatic recovery for the virtual machine.

On the Companion Media On the companion media, you will find a directory called \Chapter Materials\Scripts\Cluster. Inside the directory there are two files: Stop_clussvc_script.cmd and Havm.vbs. These files are needed during the configuration of Virtual Server 2005 R2 host cluster nodes. A listing of the script is also included in the Virtual Server Host Clustering Step-by-Step Guide for Virtual Server 2005 R2," located at %systemdrive%\Program Files\Microsoft Virtual Server\Host Clustering.

Table 5-10 lists implementation requirements prior to creating a Virtual Server 2005 R2 host cluster based on iSCSI shared storage that is supported in a production environment.

Table 5-10 Requirements for iSCSI-Based Virtual Server Host Cluster

Requirement	Description
Physical Hardware	Creation of a Virtual Server 2005 R2 host cluster supported in production requires two or more identical physical servers that are listed in the Windows Server Catalog.

Table 5-10 Requirements for iSCSI-Based Virtual Server Host Cluster

Requirement	Description
Operating System	Windows Server 2003 Enterprise Edition (SP1 or R2). Windows Server 2003 Datacenter Edition (SP1 or R2).
iSCSI	Microsoft iSCSI Software Initiator 2.0 or later version.
iSCSI Quorum and Shared Disks	iSCSI Quorum and Shared Disks targets must be created prior to configuring the cluster nodes. The Quorum disk must be at least 50 MB to satisfy Microsoft Cluster Server requirements. The Shared disk must be sized to contain virtual machine VHD files.
Network Adapters	Three network adapters must be added and configured for the Public, Private, and iSCSI networks on each Virtual Server 2005 R2 host cluster node.
Active Directory	Virtual Server 2005 R2 host cluster nodes must be members of an Active Directory domain.
Cluster Service Account	A cluster service account must be created in Active Directory.
Virtual Machine Additions	Virtual Machine Additions must be installed on each virtual machine.
Support Files	Havm.vbs and Stop_clussvc_script.cmd, located on the companion media.

To deploy a two-node Virtual Server 2005 R2 host using iSCSI, you must perform the following major steps:

1. Create a shared drive for quorum and data storage using the iSCSI Initiator.
2. Configure Microsoft Cluster Server on each Virtual Server 2005 R2 host.
3. Configure both Havm.vbs and Stop_clussvc_script.cmd on each Virtual Server 2005 R2 host.
4. Configure a cluster disk resource, resource group, and resource script.
5. Configure a virtual machine on one of the Virtual Server 2005 R2 hosts.

Important For a more detailed list of limitations and requirements, refer to the Virtual Server Host Clustering Step-by-Step Guide for Virtual Server 2005 R2 SP1.

Configuring the iSCSI Shared Disks

Follow these steps to configure virtual machine cluster node access to iSCSI shared disks:

1. Install the Microsoft iSCSI Initiator software on the first Virtual Server 2005 R2 host.
2. Click Start, click All Programs, click Microsoft iSCSI Initiator, and then click Microsoft iSCSI Initiator again.
3. Click the Discovery tab, and in Target Portals, click Add.
4. Enter the name or IP address of the server where the target iSCSI drive is defined.
5. Click the Targets tab to display a list of disk targets.
6. Select Quorum and click Log On.
7. Select Automatically Restore This Connection When The System Boots And Enable Multipath if you have multipath software installed.
8. Repeat steps 6 and 7 for the Shared target, and then click OK.
9. In the Disk Management MMC, format each disk with a single partition, using drive letter Q for the quorum disk and drive letter S for the Shared disk.
10. Shut down the Virtual Server 2005 R2 host.
11. Repeat steps 1 through 8 for the second Virtual Server 2005 R2 host.
12. In the Disk Management MMC, set the Quorum drive letter to Q and the Shared drive letter to S.

Configuring Microsoft Cluster Server on the First Virtual Server Host

Follow these steps to configure Microsoft Cluster Server on the first virtual server host:

1. Log in to the first Virtual Server 2005 R2 host with Domain Administrator credentials.
2. Click Start, click All Programs, click Administrative Tools, and then click Cluster Administrator.
3. When prompted with the Open Connection To Cluster dialog box, select Create New Cluster in the Action drop-down list.
4. Review the information list on the New Server Cluster Wizard Welcome page, and then click Next.
5. In the Cluster Name text box, type a name for the cluster and then click Next.
6. In the Computer Name text box, type the computer name of the virtual machine that is the first node in the cluster.
7. Click Next.
8. Remedy any errors found in the Analyzing Configuration step and then re-analyze. If there are no further errors, click Next.

9. In the IP Address text box, type an IP address on the public network that will be used to manage the cluster and click Next.
10. In the User Name text box, type the name of the cluster service account that you created in Active Directory.
11. In the Password text box, type the password for the cluster service account.
12. In Domain, select your domain name from the drop-down list and then click Next.
13. Review the Summary page to verify that all information used to create the cluster is correct.
14. Click Quorum, select Disk Q: from the drop-down list, and then click OK.
15. Click Next.
16. Once the cluster creation is complete, click Next.
17. Click Finish to complete the installation.

Configuring Microsoft Cluster Server on the Second Virtual Server Host

Installing Microsoft Cluster on the second Virtual Server 2005 R2 host is again a quick process because the cluster configuration already exists. Additional cluster nodes just have to be added to the existing cluster.

When adding subsequent nodes, leave the first cluster node and all shared disks turned on, and power-up additional nodes. The cluster service will control access to the shared disks to eliminate any chance of corruption. Follow these steps to configure the second node (and any subsequent node) in the cluster:

1. Open Cluster Administrator on the first cluster node.
2. Click File, click New, and then click Node.
3. On the Add Cluster Computers Wizard Welcome page, click Next.
4. In the Computer Name text box, type the computer name for the second cluster node and then click Add.
5. Click Next.
6. Remedy any errors found in the Analyzing Configuration step and then re-analyze. If there are no further errors, click Next.
7. Type the password for the cluster service account, and then click Next.
8. Review the summary information that is displayed for accuracy, and then click Next.
9. Review any warnings or errors encountered during cluster creation, and then click Next.
10. Click Finish to complete the installation.

Configuring the Shutdown Script for Virtual Server Host Cluster Nodes

Because Virtual Server 2005 R2 is not a cluster-aware application, you have to ensure that the cluster service shuts down and all virtual machines are failed over prior to a Virtual Server Host shutdown. Follow these steps to configure the shutdown script for the Virtual Server 2005 R2 host cluster nodes:

1. In the root directory of the local hard disk on each Virtual Server 2005 R2 host, copy the Stop_clussvc_script.cmd file from the companion media.
2. Click Start, click Run, and then type **gpedit.msc**.
3. Click Enter.
4. Navigate to Local Computer Policy, click Computer Configuration, click Windows Settings, and then click Scripts.
5. In the right-hand pane, double-click Shutdown, and click Add.
6. In the Script Name text box, type the fully qualified path name of the batch file, and then click OK twice.

Configuring the Disk Resource, Resource Group, and Havm.vbs Script

Follow these steps to configure the cluster disk resource, resource group, and cluster control script:

1. On the first Virtual Server 2005 R2 host, click Start, click Control Panel, click Administrative Tools, and then click Cluster Administrator.
2. In Cluster Administrator, create a new resource group and name it **Group0**. If you want to specify a Preferred Owner for the group, specify the node on which you want the guest to run most of the time.
3. In Cluster Administrator, create a new disk resource, or use the appropriate disk resource if it has already been created. Verify that it is the Shared disk configured as a Physical Disk Resource with no dependencies, assigned to resource group Group0, and both cluster nodes are listed as Possible Owners.
4. With Group0 online, create a folder on the Shared disk called **GuestVM1**.
5. On each Virtual Server 2005 R2 host cluster node, create a folder on the local disk in %systemroot%\Cluster and copy the Havm.vbs script into it from the companion media.

Important If you want to create and fail over multiple virtual machines independently, you have to configure each guest in its own resource group. If you want to fail over certain virtual machines together, you need to configure them in the same resource group.

Creating a Virtual Machine on the First Virtual Server Host

Follow these steps to configure the virtual network and virtual machine on the first Virtual Server 2005 R2 host cluster node:

1. Click Start, click All Programs, click Microsoft Virtual Server, and then click Virtual Server 2005 R2 Administration Website.
2. In the navigation pane, under Virtual Networks, click Create.
3. In the Virtual Network Name text box, type in a name for the cluster network.
4. In Network Adapter On Physical Computer, select the network adapter associated with the public network, and then click OK.
5. In the navigation pane, under Virtual Networks, click Configure, and then click View All.
6. In Virtual Networks, click on the virtual network you created, and then click Edit Configuration.
7. Copy the fully qualified path of the .vnc file.
8. Open Explorer, and paste the fully qualified path of the .vnc file (without the filename) into the address bar.
9. Right-click the cluster network name you just created, and then click Cut.
10. In Explorer, navigate to the GuestVM1 folder on the Shared disk and paste the .vnc file.
11. Open the Virtual Server 2005 R2 Administration Website.
12. In the navigation pane, under Virtual Networks, click Add.
13. In the Existing Configuration (.vnc) File text box, type the fully qualified path to the new .vnc file that you created in the Shared disk GuestVM1 folder and then click Add.
14. Copy an existing virtual machine into the Shared disk GuestVM1 folder.
15. In the navigation pane, under Virtual Machines, click Add.
16. In the Fully Qualified Path To File text box, type the fully qualified path to the virtual machine .vmc file and then click Add.
17. In the virtual machine Configuration pane, click Network Adapters.
18. In the Virtual Machine Network Adapter Properties pane, in the Connected To drop-down box, select the cluster network that you created and then click OK.

Completing the Virtual Machine Configuration on the Second Virtual Server Host

Follow these steps to complete the configuration of the virtual machine on the second Virtual Server 2005 R2 host:

1. On the second Virtual Server 2005 R2 host, click Start, click All Programs, click Administrative Tools, and then click Cluster Administrator.
2. Move Group0 to the second Virtual Server 2005 R2 host cluster node.
3. Open the Virtual Server 2005 R2 Administration Website.
4. In the navigation pane, under Virtual Networks, click Add.
5. In the Existing Configuration (.vnc) File text box, type the fully qualified path to the .vnc file located on the Shared disk in the GuestVM1 folder and then click Add.
6. In the navigation pane, under Virtual Machines, click Add.
7. In the Fully Qualified Path To File text box, type the fully qualified path to the virtual machine .vmc file and then click Add.
8. Open Cluster Administrator, and create a new script resource called **GuestVM1Script**.
9. Configure the resource as a Generic Script resource, assign it to Group0 with Possible Owners listing both cluster nodes, and add a Shared disk as a resource dependency.
10. In the Script Filepath text box, type **%windir%\Cluster\Havm.vbs**.
11. Click Start, and then click Run.
12. Type '**cluster res "Guest1Script" /priv VirtualMachineName=*GuestVM1***', replacing *GuestVM1* with the name of the virtual machine that you added, and then press Enter.
13. Open Cluster Administrator and bring Group0 online.
14. Open the Virtual Server 2005 R2 Administration Website.
15. Verify that the virtual machine is in the Running state.

You can now verify that the virtual machine fails over to the first Virtual Server 2005 R2 host cluster node. To do this, open the Cluster Administrator and choose the Move Group option for the Group0 resource group. You should see the Owner field change when the virtual machine has failed over.

Summary

There are many advanced features in Virtual Server 2005 R2 that you can leverage to optimize virtualization infrastructure deployments. If you are going to create complex testing, support desk, or user-training scenarios, use differencing disks and undo disks to enable quick provisioning of new virtual machine configurations with the ability to roll back to the baseline state. When you need to reduce the size of dynamically expanding disks, use defragmentation and precompaction prior to the VHD compaction tool to minimize the size of compacted virtual hard disks. Configure the Microsoft Loopback Adapter to create isolated network connections between a Virtual Server 2005 R2 host and its hosted virtual machines. For cluster-aware applications running within virtual machines, use a virtual machine cluster to minimize downtime from virtual machine failures. In the case of non–cluster aware applications, deploy high-availability Virtual Server 2005 R2 host clusters to reduce planned and unplanned downtime.

Additional Resources

The following resources contain additional information related to the topics in this chapter:

- Knowledge Base article 311272, "The DevCon command-line utility functions as an alternative to Device Manager," at *http://support.microsoft.com/kb/311272*
- White paper, "Virtual Hard Disk Image Format Specification," at *http://www.microsoft.com/windowsserversystem/virtualserver/techinfo/vhdspec.mspx*
- White paper, "Using iSCSI with Virtual Server 2005 R2," at *http://go.microsoft.com/fwlink/?LinkId=55646*
- White paper, "Virtual Server Host Clustering Step-by-Step Guide for Virtual Server 2005 R2," in %systemdrive%\Program Files\Microsoft Virtual Server\Host Clustering

Chapter 7

Best Practices for Configuration and Performance Tuning

In this chapter:

This chapter provides recommendations and best practices to configure a Microsoft Virtual Server 2005 Release 2 (R2) Service Pack 1 (SP1) host and virtual machines to optimize performance. The chapter covers Virtual Server 2005 R2 SP1 Administration Website configuration, host and virtual machine performance tuning, and operational considerations. Performance tuning modifications are included for processor, memory, display graphics, hard disk, and networking components.

Configuring the Administration Website

The Virtual Server 2005 R2 SP1 default Administration Website configuration is designed for generic deployments. Additional tuning is required to provide an optimized experience for managing hosts and virtual machines. This section reviews configuration options for Virtual Server 2005 R2 SP1 search paths, default configuration folder location, and remote control.

Configuring Search Paths

The Virtual Server Administration Website is the primary interface to manage the configuration of virtual machines, virtual hard disks, and virtual networks on any Virtual Server host in your network. As a browser-based tool, it offers flexibility and a few limitations. When creating a new virtual machine, for example, you can enter a fully qualified path to an existing virtual hard disk or create a new virtual hard disk and provide the fully qualified path to the location

to store the .vhd file. Unfortunately, the Virtual Server Administration Website does not provide the ability to browse the file system to select the fully qualified path. Therefore, before you enter a path to a file, you will probably identify and copy the fully qualified path in Explorer, paste it into the input box, and add the name of the file that you want to read or write to.

To simplify this process, the Virtual Server 2005 R2 Administration Website provides a way to specify search paths that will be parsed and cached for display. The Administration Website applies filters based on the action that you are performing, and it displays only the relevant files in the appropriate drop-down boxes. Figure 7-1 shows the Search Paths configuration screen.

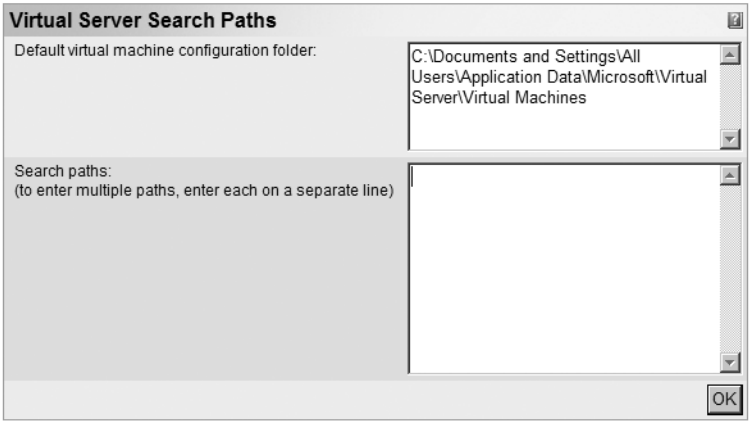

Figure 7-1 Search paths configuration screen

For example, if you are attempting to select a CD-ROM ISO image file to attach to a running virtual machine, the only ISO files that are presented are the ones copied during Virtual Server installation. By default, these are displayed because the directory is automatically added to the search paths list at installation time.

Best Practices Create a directory on the Virtual Server host to store all the files that are commonly used by virtual machines (ISO, VFD, and so on). You should use subdirectories to organize the different types of files and simplify selection.

Best Practices Add all directories in which you store virtual machine files to the Virtual Server Search Paths. Once this is configured, files in the specified directories will automatically be parsed and displayed in any drop-down list on the Web site. This allows you to select a file rather than typing the fully qualified path.

Modifying the Search Paths Configuration

To configure the search paths options on your server, follow these steps:

1. Determine the paths that you would like to add to the Administration Website.
2. Open the Virtual Server 2005 R2 Administration Website.
3. In Virtual Server, click Server Properties.
4. Click Search Paths to open the Search Paths configuration page, as shown in Figure 7-1.
5. Type the search paths (one per line) as full path statements, as shown in the following example:

```
C:\ISOs
D:\Virtual Machines
```

6. Click OK to save the search paths entered.

Configuring the Default Virtual Machine Configuration Folder

The virtual machine configuration folder defines the default storage location for any new virtual machine. Table 7-1 lists the default location for the virtual machine configuration folder for various operating systems.

Table 7-1 Virtual Machine Configuration Folder Defaults

Operating system	Default location
Microsoft Windows XP and Windows Server 2003	C:\Document and Settings\All Users\Application Data\Microsoft \Virtual Server\Virtual Machines
Windows Vista	C:\Users\Public\Documents\Shared Virtual Machines

If you create new virtual machines and specify only the name of the virtual machine instead of a full path to the configuration file (.vmc), Virtual Server 2005 R2 creates a subdirectory using the name of the virtual machine and stores the .vmc file at that location. Virtual Server 2005 R2 stores the save state file (.vsv) and any undo disk files (.vud) in the same directory as the .vmc file. Because the default folder location is on the system volume, it has the potential to cause disk space issues that can significantly affect Virtual Server 2005 R2 performance.

Best Practices Modify the default virtual machine configuration folder location to store virtual machines on a volume other than the system volume. When you change this path, the folder access control is reset to the security configuration specified in the Virtual Server 2005 R2 Administration Website.

Modifying the Default Virtual Machine Configuration Folder

To modify the default folder for virtual machines, follow these steps:

1. Determine the path that you would like to use as the new virtual machine default folder.
2. Open the Virtual Server 2005 R2 Administration Website.
3. On the left navigation menu, click Server Properties.
4. Click Search Paths. You will see the Search Paths configuration screen shown in Figure 7-1.
5. In the Default Virtual Machine Configuration Folder text box, type the new default folder location as full path statements, as shown in the following example:

   ```
   D:\Shared Virtual Machines\
   ```

6. Click OK to save the settings.

Direct from the Source: Beware of Automatic ACL Changes

When you change the default virtual machine configuration folder to a new location, or when you add or remove an entry in the Virtual Server 2005 R2 Security Settings, the default virtual machine configuration folder specified and all subdirectories will have the access control lists (ACLs) reset to the current security configuration of the Virtual Server site. You will not receive a warning that this is going to occur.

The ACLs of the default virtual machine configuration folder root are completely replaced, and the subdirectories are reset in an overlay mode. If there is a group with ACLs defined on a subdirectory of the default virtual machine configuration folder and that group is being used in a security setting in Virtual Server, that ACL entry will be overwritten with the ACL settings defined in the Virtual Server 2005 R2 security setting.

Joseph Conway
Support Escalation Engineer, Virtualization

Enabling Virtual Machine Remote Control

Microsoft Virtual Machine Remote Control (VMRC) is disabled by default when you install Virtual Server 2005 R2. This ensures that the default installation of Virtual Server has a reduced remote attack surface. To remotely manage a virtual machine from a power-on state, you need to enable VMRC. VMRC allows access to all virtual machines on the Virtual Server 2005 R2 host based on access permissions. Unless you provide the name of a specific virtual machine, an administrative screen will be displayed containing thumbnail snapshots of all the virtual machines' current video buffers.

When you enable VMRC, there are a series of options that you can configure, as shown in Table 7-2.

Table 7-2 VMRC Configuration Options

Option	Description
TCP/IP address	TCP/IP address that VMRC uses for communications.
TCP/IP Port	TCP port number that VMRC uses for communications. The default port number is 5900.
Default Screen Resolution	Screen resolution that the VMRC client uses when establishing a remote session with a virtual machine.
Authentication	Authentication Protocol that is used for authenticating access to the VMRC client: Automatic, NTLM, or Kerberos.
Disconnect idle connections	Amount of time in minutes that the VMRC server waits with no activity before disconnecting the VMRC client session.
Multiple VMRC Connections	Enables the ability for a VMRC client session to allow more than one user to connect to a virtual machine.
SSL 3.0/TLS 1.0 encryption	Enables or disables the use of Secure Sockets Layer (SSL) or Transport Layer Security (TLS) encryption for the VMRC sessions.
SSL 3.0/TLS 1.0 certificate	Required information to configure the certificate used for establishing the encrypted VMRC session.

There are two interfaces to the VMRC protocol: an ActiveX control and a Windows client. The ActiveX control is the interface presented by the Virtual Server 2005 R2 Administration Website. The Windows VMRC Client is accessible from the Virtual Server program menu option. The configuration options in Table 7-2 affect both VMRC interfaces. You should consider each of the best practices in the following sections to modify the configuration of your Virtual Server 2005 R2 installations.

Enabling VMRC

To enable VMRC after installing Virtual Server 2005 R2 to allow remote management of virtual machines, follow these steps:

1. Open Virtual Server 2005 R2 SP1 Administration Website in an Internet Explorer browser window.
2. On the Virtual Server menu, click Server Properties.
3. In the Properties window, click Virtual Machine Remote Control (VMRC) Server.
4. To enable VMRC on this server, select the Enable check box as shown in Figure 7-2.

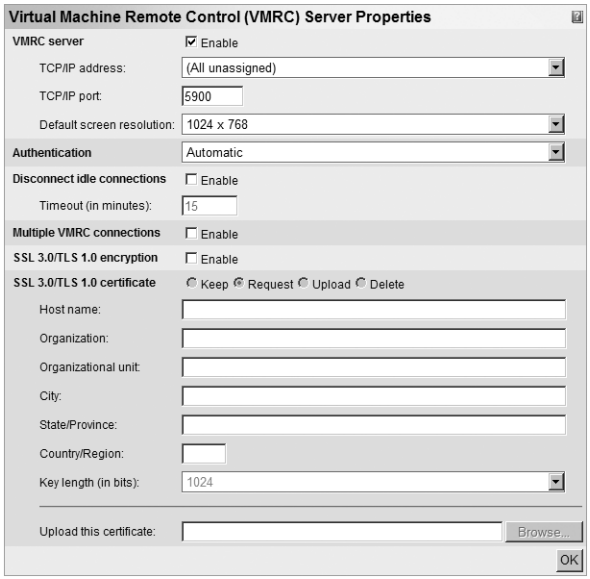

Figure 7-2 VMRC options screen

5. Optionally, disable idle connections by selecting the Enable check box in the Disconnect Idle Connections section.
6. Optionally, enable multiple VMRC connections by selecting the Enable check box in the Multiple VMRC Connections section.
7. Click OK.

Best Practices Configure VMRC to listen only on a specific TCP/IP address if the host has multiple network adapters. This ensures that all VMRC traffic goes only across a single network card and a single TCP/IP address. This configuration makes it easier to troubleshoot any issues with VMRC.

Best Practices Change the default port for VMRC. Changing the default port provides additional protection to the VMRC service against denial of service attacks or other security threats. Changing the default port forces you to specify the port number as part of the query string in the VMRC client.

Best Practices Configure the authentication setting of VMRC to Kerberos to ensure that only Active Directory domain member servers can remotely manage the Virtual Server 2005 R2 host. This configuration provides an additional layer of security from remote systems that are not members of the Active Directory domain. Enabling this feature requires contacting a domain using Kerberos to authenticate the remote user session.

Best Practices Only enable multiple VMRC connections when you need the ability for multiple people to connect to a virtual machine concurrently. Scenarios might include debugging, training, or installation support purposes.

Best Practices Enable and configure SSL/TLS to protect the Internet Information Services (IIS) and VMRC network traffic when you enable basic authentication. By default, the Administration Website pages are not encrypted during transfer. When Windows authentication is used, user IDs and passwords are encrypted. Refer to Chapter 6, "Security in Depth," for more information on securing Virtual Server and configuring SSL/TLS.

How to Obtain the Best Host Performance

Configuring your Virtual Server host to obtain the best performance requires focusing on five key configuration areas: processor, memory, display graphics, disk subsystem, and network adapters. Using the fastest hardware components available is a good beginning, but how you combine them to obtain the optimum configuration is not always obvious. In this section, you will learn more about the five key configuration areas and best practices to obtain the optimum performance for your Virtual Server 2005 R2 host.

Maximizing Processor Performance

Virtual Server 2005 R2 is a multithreaded application that performs best on servers containing multiple processors. Processors today are single core or multiple core and come with or without virtualization hardware assistance—such as Intel Virtualization Technology (Intel VT) and AMD Virtualization (AMD-V). They can also have hyperthreaded logical processors.

Because the number of simultaneous threads is directly related to the number of processor cores that are available to execute them, the best host configuration is one that has multiple cores. To maximize the number of processors available and minimize the footprint of the server that you are using, purchasing servers with the latest quad-core processors will provide you with the best price-to-performance solution.

Virtual Server 2005 R2 SP1 now supports the processors from Intel and AMD with hardware virtualization support: Intel VT and AMD-V. Hardware virtualization-assisted processors relieve Virtual Server 2005 R2 SP1 from performing some virtualization operations in software, thereby providing performance gains. Virtual Server 2005 R2 SP1 uses virtual machine additions to tune the performance of supported Windows and Linux operating systems. Most performance gains from the current series of hardware virtualization-assisted processors are obtained when the virtual machine additions have not yet been loaded, mainly during virtual machine boot and operating system installation.

Buying servers that have hyperthreaded processor cores will provide you nominal performance improvement. Hyperthreaded processors are logical and operate well in low workload conditions, using available physical cycles to process more instructions. As the load on the physical processor cores increase, the hyperthreaded processors become starved for processor cycles, and performance of threads and processes depending on a hyperthreaded processor can be significantly affected. To ensure that a thread of execution for a virtual machine does not experience this degradation, Virtual Server does not schedule any Virtual Server threads of execution on hyperthreaded processors.

Best Practices Purchase servers with multicore Intel VT or AMD-V processors as Virtual Server 2005 R2 SP1 hosts. Quad-core systems should be the minimal multicore processor configuration. Although it's not required, you should consider disabling hyperthreading on the cores in a Virtual Server host to remove them from operating system management and monitoring cycles. If you do not do this, any workload analysis tool that determines the maximum available and utilized processing power will incorrectly include hyperthreaded processors and invalidate the calculations.

Maximizing Memory Performance

Available memory is a critical requirement in a Virtual Server 2005 R2 environment because Virtual Server uses only physical RAM to load and run virtual machines. Properly planning the memory requirements and configuration of a Virtual Server can have positive performance results for a virtual machine.

Understanding Memory Types

Most motherboards can use different types of memory, depending on the processor and chipset in use. Memory choices typically involve a tradeoff between speed and capacity. By choosing the faster memory chips, you typically reduce the maximum capacity of memory available in the system. This difference can be significant and as large as a 75-percent reduction in memory capacity. For example, the same motherboard might be able to install 128 GB of 266-MHz PC2700 memory, 64 GB of 333-MHz PC2700 memory, or only 32 GB of 400-MHz PC3200 RAM. Using the fastest RAM will dramatically reduce the amount of total RAM available and the number of virtual machines that your host can support. You should always verify the configuration with your hardware vendor to be assured that you are using the correct configuration settings.

Best Practices Determining the best practice configuration for memory in a Virtual Server 2005 R2 host is really driven by the goals of the system. If the goal is to obtain the fastest memory performance possible on the Virtual Server host, use the fastest memory available. If the goal is to obtain the best performance possible but run the maximum number of virtual machines on the host as possible, use the memory that gives you the highest capacity and attempts to compensate with other components, such as faster processors or a faster speed disk subsystem.

Understanding Memory Configuration

Memory chip performance is not the only consideration when evaluating the performance of virtual machines. Virtual machines that have too little memory allocated to them suffer from excessive amounts of memory paging to disk. Disk access is typically measured in milliseconds (10^{-3} seconds), while memory access is measured in nanoseconds (10^{-9} seconds). That makes memory access 1 million times faster than disk systems in retrieving data. Because disk access in a virtual environment has additional overhead, the actual impact on performance is even higher. Reducing the amount of memory paging to disk will increase the performance of the virtual machines.

Operating systems inside virtual machines require no less memory than on their physical counterparts. Virtual machines incur memory overhead for interfaces to the Virtual Machine Monitor (VMM), video buffer, keyboard buffer, and mouse buffer, whereas purely physical environments do not. Memory overhead varies but typical values are 32 MB of additional space over the standard memory assigned.

Physical servers are typically purchased based on a standard configuration. In the case of memory, many physical servers were purchased with more memory than the workloads required. When virtualizing the servers, it is a good time to reevaluate the actual physical server memory requirements.

Best Practices Once you have determined the actual memory required for the physical server, you should use a scaling factor when planning the amount of memory that you allocate to a virtual machine. A good value is 1.25 times the memory that you would have allocated to a purely physical machine with the additional 32 MB for overhead. This increased allocation will provide more memory for the virtual machine, increase the number of applications that can be loaded in the virtual machine's RAM, and reduce the amount of paging to disk. The formula is as follows: Virtual Machine required memory = 32 MB + (1.25 × original physical server RAM in MB).

Understanding Non-Uniform Memory Access

Another memory consideration involves the architecture of the processor and motherboard. Non-Uniform Memory Access (NUMA) is an architectural feature of modern multiprocessor platforms. NUMA architecture combines the processor, I/O bus, and memory into a "node" that is tuned for performance. These nodes are interconnected by a high-speed bus system. The processor has faster access, with lower latency and greater bandwidth to the memory contained within the node. When the server needs to access memory on another node using the system interconnect, the performance will be affected by increased latency and reduced bandwidth. Proper configuration of a NUMA-based machine allows for maximizing local memory access while minimizing memory access using the system interconnect. An improperly configured NUMA-based server can suffer from significant performance issues.

Configuration of a NUMA architecture server requires understanding the memory requests of the virtual machines that will be running in the system. To properly configure the memory on a NUMA system, you need to evenly distribute the memory assigned to each processor. This gives each processor the same size of local cache and minimizes the memory requests between nodes. Figuring out how much memory to put in the system depends on a combination of factors, including the largest memory block a virtual machine requires, the number of processors in the system, and the size of the memory sticks that the system will accept.

If you have a virtual machine that is assigned 3.6 GB of memory, you need to ensure that you have at least 4 GB of memory installed on each processor node in the NUMA system so that the virtual machine thread running on a processor will be able to have all of its memory loaded in the local node. If you have 4 processor nodes, the minimum amount of memory you should be placing in the server is 16 GB, or 4 GB per node.

Direct from the Source: NUMA Ratio

NUMA vendors have established a NUMA ratio value that describes the amount of time it takes for a node to access "remote" memory, or memory that is assigned to another node, versus its own "local" memory. Generally, performance is not affected if the NUMA ratio is between 1.0 and 1.5. Once the ratio is 3.0 or greater, performance will degrade.

On NUMA systems that have one or more nodes without memory assigned, you will find Event IDs 1100 and 1101 in the application event log when the Virtual Server service starts. These events will be logged when a NUMA configuration is not set up properly. You will also see these errors on multicore systems where memory allocation to additional cores is not defined in the Static Resource Affinity Table (SRAT) but is handled instead at the BIOS level. Please check with your hardware vendors regarding their specific NUMA configurations to understand how to properly configure the memory.

Rob Hefner
Microsoft Services Support Engineer, Virtualization

Best Practices Determine the largest block of memory that will be requested on the NUMA system, and then purchase at least that much memory per processor. Because a virtual machine can be configured with a maximum of 3.6 GB of RAM, the minimum amount of memory per processor should be 4 GB of RAM. You should evenly distribute the memory to each processor to maximize local node use of memory and reduce the number of memory calls to another node.

Increasing Display Graphics Performance

Display graphics performance has two primary areas: the performance on the host, and the performance of the virtual machines. Increasing graphics performance on the host provides a better user experience when interacting at the console of the Virtual Server 2005 R2 host. Increasing graphics performance of virtual machines provides a better user experience when interacting with the Virtual Machine Remote Control (VMRC) console application.

Increasing the display graphics performance involves adjusting the display configuration and the visual effects configuration of the hosts and virtual machines. Windows display adapter drivers have an advanced setting that controls the level of hardware acceleration that is being used. The value ranges from No hardware acceleration to Full hardware acceleration. Most Windows Server installations do not automatically set the acceleration level to Full, preventing the maximum performance for the display subsystem.

Best Practices Enable Full hardware acceleration on the Virtual Server host and every virtual machine to obtain the best display adapter performance. In rare instances, increasing the hardware acceleration level will decrease performance. In these instances, an older display graphics driver that requires an update to the latest version is usually the source of the problem.

Adjusting the Display Hardware Acceleration

To adjust the display hardware acceleration, follow these steps:

1. On Windows XP and Windows Server 2003, right-click the desktop and select Properties.

   On Windows Vista, right-click the desktop, select Personalize, and then select Display Settings.

2. Click the Settings tab, and then click the Advanced button.
3. Click the Troubleshoot tab and you will see a Hardware Acceleration slider bar dialog box as shown in Figure 7-3.

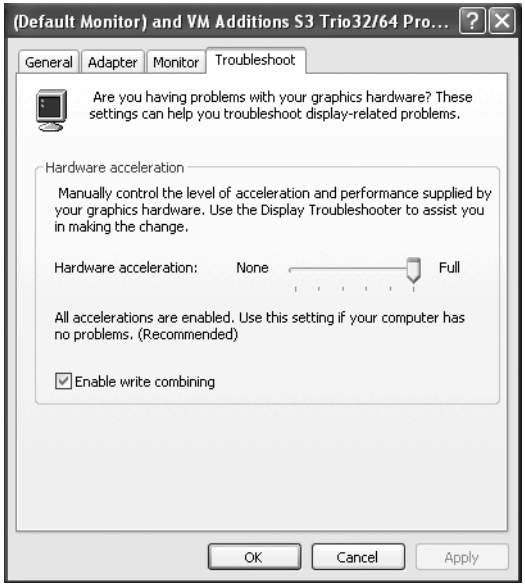

Figure 7-3 Hardware acceleration slider bar

4. Move the slider to the right side where it says Full, and click OK.

Increasing VMRC Performance

VMRC allows you to remotely connect to the Virtual Server host and view the screens of virtual machines to which you have access. The Virtual Server service (Vssrvc.exe) contains the VMRC server-side interface that communicates with the VMRC client-side component. The default port that the VMRC service listens on is TCP port 5900.

The VMRC interface does not use the on-board display graphics adapter to generate virtual machine screens. All VMRC operations are performed purely in software. Therefore, one way to increase the graphics performance of VMRC sessions is to use faster processors and network adapters in the host.

You can also improve the performance across the network by enabling the option to use reduced colors. Enabling reduced colors can be accomplished two ways: enabling the option from the Virtual Server Administration Website, or enabling the option from the VMRC Windows client. When enabled from the Administration Website, all VMRC sessions to the Virtual Server configured to use reduced colors are affected. When enabled from the VMRC client, only the active server connection is affected.

Enabling Reduced Colors from the Administration Website

To enable reduced colors for all VMRC sessions to a Virtual Server host, follow these steps:

1. Open the Administration Website on the desired Virtual Server host.

2. Select Website Properties from the left menu.
3. In the Virtual Machine Remote Control Properties section, select the Use Reduce Colors check box and then click OK.

Enabling Reduced Colors from the VMRC Windows Client

To enable reduced colors for a specific VMRC session to a Virtual Server host, follow these steps:

1. Click the Start button, select Programs, select Microsoft Virtual Server, and click Virtual Machine Remote Control Client.
2. Select the Reduce Colors check box as shown in Figure 7-4.

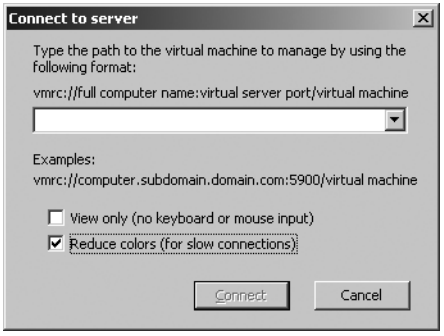

Figure 7-4 VMRC dialog box

3. Type the name of the Virtual Server to manage in the Path box, and click Connect.

Best Practices Enable reduced colors in the VMRC client interface when connecting to a Virtual Server host across a slow wide area network (WAN) connection. Enable reduced colors on the Web properties of a Virtual Server host if all administration will be performed over a slow WAN connection.

Optimizing Hard Disk Performance

Virtual Server host scalability is heavily dependent on the disk subsystem. As you add more virtual machines to a host, the disk I/O workload increases. A single virtual machine performing heavy disk I/O can adversely affect the performance of other running virtual machines. In addition, applications that are running on the Virtual Server 2005 R2 host can affect disk performance.

Evaluating Virtual Server Host Applications that Are Affecting Disk Performance

Applications that can affect a Virtual Server host disk performance should be eliminated or reconfigured to minimize the effects on disk performance. Antivirus software is an example of a common application that is installed on Virtual Server hosts. Antivirus software is typically implemented as a disk filter driver that intercepts all calls for read access and writes to the hard disk and that scans the information for viruses before allowing the operation to complete. Antivirus software typically targets executables and other file types that can present a threat to the host operating system.

Virtual Server services and associated file extensions are not excluded by default from most antivirus applications. Most antivirus applications allow you to exclude file extensions or processes from virus scans. If you exclude the file extension, it excludes any application that might be reading and writing to those files, which might include a virus or Trojan horse. However, if you exclude processes, any other application that attempts to open the files would be scanned and the potential for catching a virus or Trojan horse is much higher.

Best Practices You should configure the antivirus application to exclude file extensions or processes. Using the process exclusion method rather than the file exclusion method is recommended because it provides better protection. When configuring the antivirus software to exclude the Virtual Server processes, you should exclude the Virtual Server service (Vssrvc.exe) and the Virtual Machine Helper service (Vmh.exe).

If your antivirus application does not support excluding processes, you should add .vhd, .vmc, .vud, .vfd, .vsv, and .vnc file extensions to your antivirus file exclusion list so that they are not scanned.

Understanding Disk Hardware Performance

Obtaining the best disk performance for your virtual machines requires the use of high-speed disks and spreading the disk I/O load over as many spindles as possible. The speed of the disk is directly related to how fast data can be read from and written to the disk. Hard drives typically come in speeds of 4200, 5400, 7200, 10,000, and 15,000 revolutions per minute (RPM). The most common drive speed today is the 7200-RPM drive.

Hard disk platters are arranged in concentric circles called *tracks*. Each track is divided into sectors that look like smaller arcs. As the platter spins, the read/write head is positioned over the track where sectors are located. The faster the platter spins, the faster the read/write head can access the sector, increasing throughput.

Best Practices You should use 10,000-RPM or faster drives in the Virtual Server host to minimize the data read/write times for virtual machines. Using a 10,000-RPM drive rather than a 7200-RPM drive significantly increases the number of read and write operations performed per minute.

Understanding How Disk Types Affect Performance

Disk speed is only one part of the equation. The type of drive is also very important. Drive types available today include Parallel-ATA, Serial-ATA, Serial Attached SCSI (SAS), and SCSI. All drive types have different performance specifications, and most even have different grades of drives, with higher throughput capabilities as the grades and prices increase. Table 7-3 shows a comparison of the performance ratings of standard SATA, SAS, and SCSI drives currently available.

Table 7-3 Drive Performance Comparison

Drive type	Throughput	Queuing
SATA	2.4 gigabits/second per drive	NCQ
SAS	6 gigabits/second per drive	TCQ
SCSI	2.5 gigabits/second per shared bus	none

Drives also operate using different protocols. Parallel Advanced Technology Attachment (PATA) drives must complete a read or write request before they will perform the next read or write in the queue. Serial Advanced Technology Attachment (SATA), Small Computer System Interface (SCSI), and Serial Attached SCSI (SAS) drives can queue multiple requests and make intelligent decisions about which sequence the operations should be performed in. The latest SATA drives use a method called Native Command Queuing (NCQ), while SCSI and SAS drives use a similar method called Tagged Command Queuing (TCQ). Both methods are designed to increase performance by allowing an individual hard disk to queue more than one I/O request at a time and dynamically modify the order in which the operations are performed.

Figure 7-5 shows the comparison of two disk operations accessing different tracks with and without command queuing. Without command queuing, the read/write head has to perform the operations in the order they were submitted into the queue. It might have to bypass the track that the second operation needs in order to access the track for the first operation. Then it would have to complete additional revolutions and head movement to perform the second operation, decreasing efficiency. With command queuing, operations can be optimized to perform the second operation and then the first operation. This flexibility reduces disk latency.

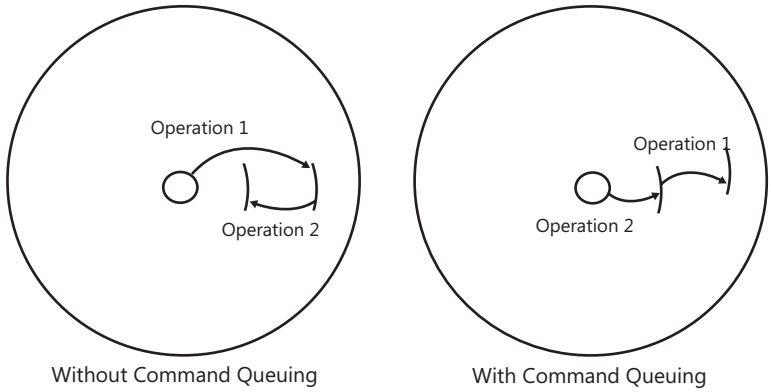

Figure 7-5 Command queuing comparison

Best Practices You should use the SATA or SAS drive type in the Virtual Server 2005 R2 host to obtain the benefits of command queuing. Although 10,000-RPM or faster drives are recommended, the exact drive type and speed will be driven by your available budget and, potentially, the original equipment manufacturer (OEM) contracts or standards that are in place.

Understanding Disk Drive Configuration

Designing a disk drive configuration that provides the best performance is dependent on the workload and the number of virtual machines that will be running on the Virtual Server 2005 R2 host. Running one virtual machine on a single dedicated spindle will provide good performance. As the number of virtual machines increases, so will the disk activity, and a single drive will no longer be able to provide acceptable read/write performance. Creating a disk array is the best way to spread the disk I/O load across multiple spindles. Redundant Array of Inexpensive Disks (RAID) level 10 is the fastest redundant disk subsystem in regular use today. RAID 10 is achieved by creating a mirrored set (RAID 1) of striped disks (RAID 0).

Storage area networks (SANs) are disk systems that have high-speed connections to drive arrays. SANs have software interfaces that allow the disk space to be combined into logical unit numbers (LUNs) and quickly reconfigured. Host bus adapters (HBAs) provide the high-speed connection between the host and the disk array. Most HBAs use fiber-optic cable connections called fiber channel.

Internet SCSI (iSCSI) is a network protocol that allows data transfer using the SCSI protocol over TCP/IP networks. iSCSI requires only an Ethernet network adapter to operate. iSCSI does not require expensive HBAs or storage protocols such as Fibre Channel, and it does not require SCSI disks to be used on the target system. This allows iSCSI to provide inexpensive access to centralize storage.

iSCSI uses a client/server metaphor for communication The iSCSI client is called an *initiator*, and the iSCSI server is called a *target*. An iSCSI initiator is a client device that connects to an iSCSI target, providing block-level access to its disk storage. One limitation of an iSCSI initiator/target system is that only one iSCSI initiator can talk to a specific iSCSI target at a time.

Best Practices You should consider a SAN that provides the redundancy of RAID 10 configurations, iSCSI target capability, and the ability to use high RPM queued I/O hard drives. Selecting one that supports SATA and SAS hard drives in the same enclosure will provide you with the most flexibility. When creating the RAID 10 disk array, you should use as many spindles as feasible to distribute the I/O load.

Optimizing Network Performance

Virtual Server shares the host's physical network adapters with virtual machines. Networking performance of the host and the virtual machines is affected by the number of virtual machines sharing an adapter, the speed of the adapter, and the adapter configuration settings. This section describes common issues involved with configuring networking on the physical and virtual machines and best practice–based solutions.

Understanding Virtual Networks and Adapters

The Virtual Machine Network Services (VMNS) driver provides the interface between the virtual networks and the physical network adapters in the host. VMNS redirects packets to the correct virtual network and attached virtual machine network adapter. Virtual networks can be bound only to a single physical network adapter at a time. One or more virtual machines are assigned to a virtual network, and the combined network traffic of the assigned virtual machines is transmitted over the single physical network adapter. Sharing a physical network adapter with multiple virtual machines can affect network performance. Installing multiple network adapters in the Virtual Server host allows you to distribute the virtual networks load and performance effects across physical interfaces.

The virtual machine emulated network adapter was selected for universal driver availability in multiple operating system releases from multiple vendors. However, this choice of network adapter reduced the available advanced features found in more recent adapters such as the following features:

- TCP/IP offloading features (checksum, segmentation, and so on)
- Jumbo frame support
- Flow Control
- Teaming
- Quality of Service (QoS) offloading

Leaving these features enabled on the physical network adapter that will be used for virtual machine traffic can potentially cause data corruption, traffic loss, and reduced throughput.

Best Practices You should dedicate a network adapter for host traffic on every Virtual Server host. This arrangement prevents the virtual machine traffic from affecting Virtual Server management tasks. This is accomplished by unbinding the VMNS driver from the physical network adapters that will be the dedicated host network adapter.

Best Practices You should dedicate network adapters for virtual machine traffic on every Virtual Server host. This arrangement prevents the Virtual Server management traffic from affecting the virtual machine traffic. This is accomplished by unbinding all services, protocols (including TCP/IP), and drivers listed in the network properties dialog box except for the VMNS driver.

Best Practices You should disable hardware acceleration features of the host physical network adapter for all virtual machine dedicated network adapters. The virtual machine emulated network adapter does not provide support for these advanced features, and leaving them on will decrease performance and potentially cause data corruption.

Optimizing Virtual Machine Performance

Virtual machine performance can be affected by different variables, including the performance of the host, the configuration options for the operating system, the type and configuration of the selected virtual hardware in the virtual machine, and how resources are allocated to the virtual machine. This section reviews these component issues and the best-practice solutions for minimizing their effects.

Virtual Machine Additions

Virtual machine additions are features that improve the performance and integration of virtual machines by installing a series of drivers in the virtual machine. Driver updates are included for the mouse, keyboard, video, and SCSI systems. However, virtual machine additions are available only for a certain subset of Windows and Linux operating systems. They are installed in the virtual machine after the Windows or Linux operating system is installed. After additions have been installed, new integration features are enabled.

Best Practices You should install the virtual machine additions as soon as possible after the operating system has been installed. This approach allows you to take advantage of the performance improvements and integration features while you are finishing the configuration of the virtual machine.

Best Practices You should update the virtual machine additions on any pre-existing virtual machines or when you migrate virtual machines from Virtual PC to Virtual Server. By updating the additions to the latest version, you ensure the best performance and the latest additions features. You should use the latest additions version available for Virtual PC or Virtual Server.

Understanding Processor Resource Allocation

Virtual Server manages processor allocation to virtual machines through the CPU resource allocation settings accessible from the Virtual Server 2005 R2 Administration Website. CPU resource allocation configuration provides three settings options: relative weight, reserved capacity, and maximum capacity. Table 7-4 defines the three resource allocation settings and the allowed ranges of the values.

Table 7-4 Resource Allocation Settings

Allocation setting	Description	Range
Relative weight	Relative values assigned to virtual machines that define the amount of processing power a virtual machines receives. A virtual machine with a high relative weight obtains more processing power than a virtual machine with a low relative weight.	1-10,000
Reserved Capacity	Reserved capacity is the percentage of a logical processor that Virtual Server will guarantee is available for a virtual machine. The maximum percentage is 100.	0-100
Maximum Capacity	Maximum capacity is the percentage of a logical processor that Virtual Server will not allow a virtual machine to exceed.	0-100

By default, all virtual machines have a relative weight of 100 and a maximum logical processor capacity set to 100 percent so that the resource requirements of each virtual machine are equal and none is given preference over another.

Understanding the Resource Allocation Management Page

The resource allocation page of a Virtual Server 2005 R2 host with two processor cores is shown in Figure 7-6. For each virtual machine, the page displays the processor resource allocation settings, the system-level processor resource allocation, and a processor utilization history graph.

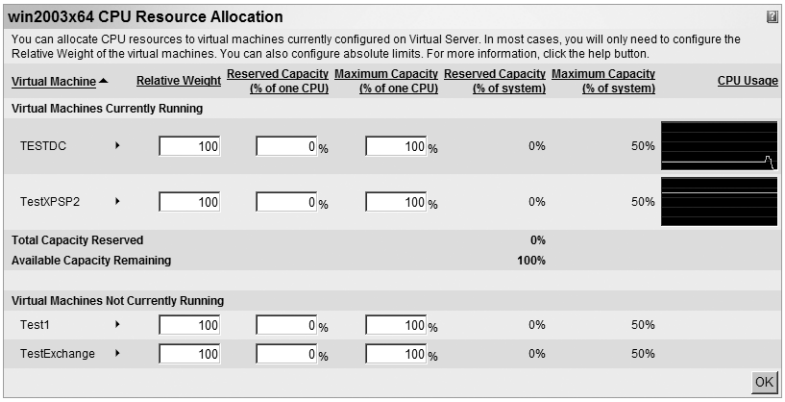

Figure 7-6 Processor Resource Allocation management page

Resource allocation has two aspects: the values that you can set on the virtual machines for relative weight, maximum capacity, and reserved capacity; and the available capacity of the host when you attempt to turn on a virtual machine. It is possible to set the reserved capacity for every virtual machine to 100 percent. Although it seems that you can oversubscribe the capacity of the processing power of the host, processor resource allocation manages the available capacity automatically for you. As you start a virtual machine that has reserved capacity set, the amount of available capacity on the system is reduced. When you attempt to start a virtual machine that has a reserved capacity allocation that is larger than the available capacity left on the system, Virtual Server will return an error and not power on the virtual machine.

The reserved and maximum capacity is calculated based on the number of processors in the host. In Figure 7-6, the host has two processors, so the maximum capacity of the system that can be allocated to a single virtual machine is 50 percent. This value is calculated by taking 100 percent and dividing it by the number of processors. But when you actually set the value for reserved capacity of the virtual machine, you are setting a percentage of the logical processor that you want to reserve. So if you want to reserve an entire logical processor for a virtual machine, you enter 100 percent for the setting, and the system will calculate the amount of system capacity that will be allocated from the available pool of capacity when you turn on the virtual machine—in this case, that would be 50 percent of the system capacity. If you set the reserved capacity of a virtual machine to 50 percent, the reserved capacity of the system would display as 25 percent, or 50 percent of the maximum value for a processor.

Resource allocation should always be part of the planning process for the placement of virtual machine workloads on a Virtual Server host. You should also revisit the current allocation on a host on a regular basis to ensure that the addition or removal of virtual machines on the host has not upset the balance of the system. Once you modify the default resource allocation approach for a host, you risk starving virtual machines for processing power. You should consider the best practices listed in this section to configure the processor resource allocation of your Virtual Server 2005 R2 host.

Best Practices You should use a tiered approach to configure processor resource allocation settings. Unless you are going to manage the resource allocation settings and modify them regularly, you should maintain the default configuration. If you have a host with virtual machines for which you want to guarantee a certain amount of processing power, you should use the reserved capacity allocation approach for those machines. Typically, you do this for a machine that has dependencies to provide services to other physical or virtual machines, such as a domain controller, or for machines that you know will have high performance requirements, such as an SQL server. If you have a host for which you want to maintain equal processing power but you know the virtual machines do not provide critical services, you should use the maximum capacity allocation to limit the effect they will have on the other virtual machines in the system.

Understanding Virtual Machine Graphics Performance

Graphics performance inside a virtual machine is dependent on the emulated graphics card. Some advanced features that are easily handled by a hardware graphics adapter can cause screen repainting issues in a virtual machine and cause the virtual machine screen refreshes to be slow. This effect is most noticeable on a Windows client operating system such as Windows XP or Windows Vista, where the visual experience uses advanced graphics features such as shadowing.

To obtain the best repaint and refresh user experience in virtual machines, you have to tune the virtual machine user interface to provide best performance instead of best user experience. By default, the user interface experience is managed by the Windows operating system. You can modify the default and adjust for best performance.

Best Practices You should adjust the Windows visual interface settings to use a "best performance" setting instead of letting Windows adjust the settings to achieve the best user experience. This is required on the Virtual Server 2005 R2 host as well as every virtual machine.

Configuring the Windows User Interface for Best Performance

To adjust the default Windows user interface to obtain the best performance, follow these steps:

1. Click the Start button, select Control Panel, and choose System.
2. Click the Advanced tab and then the Performance button. The Performance Options dialog box will be displayed as shown in Figure 7-7.

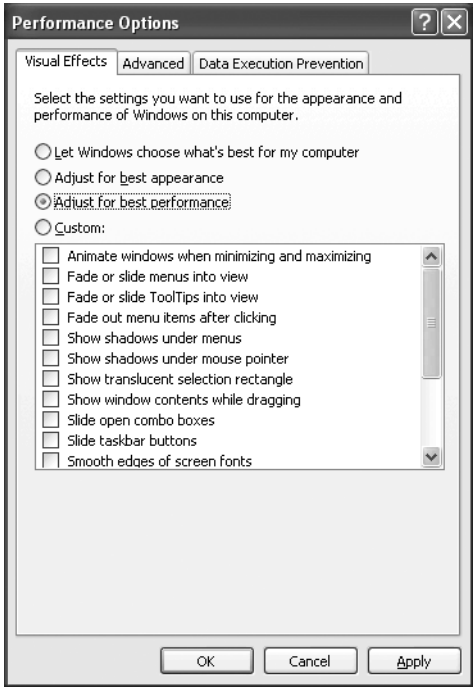

Figure 7-7 Visual effects Performance Options dialog box

3. Select the Adjust For Best Performance option.
4. Click OK.

Virtual Hard Disk Performance

Virtual hard disks are stored on the physical disk as single files with a .vhd extension. The initial size of the VHD file is dependent on the type of virtual hard disk selected. You can use a fixed-size virtual hard disk or a dynamically expanding virtual hard disk. When you create a fixed-size virtual hard disk, the entire size of the drive is allocated on the physical disk as a single file. For example, if you elect to create a 10-GB hard disk, Virtual Server 2005 R2 will create a 10-GB file on the host's drive and internally structure it like a physical hard disk. It creates a master boot record and a file table, and it stores data in virtual tracks and sectors. Initial creation of a fixed-size virtual hard disk takes longer, but once the disk space allocation is complete, the file size is not modified again. A dynamically expanding virtual hard disk has the same internal structure as a fixed-size virtual hard disk, but when it is created it does not preallocate all the disk space in the file. As you write to a dynamically expanding disk and more space is needed, it allocates 2-MB chunks of space to extend the VHD file size to the maximum size of the VHD.

Fixed-size VHD files are less prone to be fragmented when created and do not have the overhead of allocation of space on the fly. Dynamically expanding disks allow you to use physical

disk space as you go instead of pre-allocating space that is not being used. Proper disk space management is required if you elect to use dynamically expanding disks. Virtual Server does not prevent you from oversubscribing the disk space on the physical server when creating a dynamically expanding VHD. Proper planning is also required when provisioning fixed-sized virtual hard disks across the network because of the amount of data that needs to be transferred.

Virtual hard disks can also be connected to two different types of adapters in a virtual machine. The type of adapter you connect defines the size limits and virtual hard disk performance. Virtual machines provide both Integrated Drive Electronics (IDE) and SCSI adapters. Virtual hard disks attached to an IDE adapter can be a maximum of 127 GB, and virtual hard disks attached to a SCSI adapter can be up to 2 TB in size.

Virtual Server 2005 R2 IDE and SCSI virtual adapters have the same characteristics as physical adapters. A virtual SCSI adapter performs faster than a virtual IDE adapter because of architecture limitations on data transfer and SCSI adapter ability to perform multiple transactions simultaneously. Overall, virtual SCSI adapters provide approximately 20 percent performance gains over an IDE adapter on a virtual machine with virtual machine additions installed. The virtual machine additions install an optimized virtual SCSI adapter driver that provide performance enhancements over the out-of-the-box Adaptec SCSI adapter driver.

Best Practices To obtain best performance, you should create virtual hard disks as fixed disks and connect them to a SCSI bus adapter. A fixed disk eliminates the dynamic allocation overhead and oversubscription concerns on the host. Attaching the fixed disk to a SCSI adapter allows you to create larger virtual hard disks and obtain approximately a 20 percent improvement in performance.

Best Practices You should use compression software to reduce the size of the fixed virtual hard disks before you attempt to transfer them over the network. Compression technologies such as ZIP and RAR (Roshal ARchive) can achieve significant size reductions on VHD files that are mostly empty space.

Operational Considerations

Using Virtual Server 2005 R2 in test, development, or production environments requires that operational standards be established to maintain efficiency. This section addresses establishing naming standards and creating and operating a library of virtual machines.

Establishing Standards

Establishing a set of configuration standards before you roll out virtualization on an enterprise basis will save you many hours of configuration changes. Standards are critical to minimizing virtual machine migration efforts between hosts, provisioning virtual machines, and making virtual machines and virtual networks easily identifiable.

Virtual machines are listed in the Administration Website according to the virtual machine configuration (.vmc) filename, and they are sorted in ascending alphabetical order. The .vmc filename is not required to match the actual computer name of the virtual machine. This approach provides both flexibility and confusion. You are allowed to specify a different name for the .vmc file than the virtual machine, giving you flexibility for sorting and grouping in the user interface. However, you must maintain a mapping of the .vmc name to the machine name. The virtual machine configuration filename is required to be unique on a single host, but duplicate names can exist on other Virtual Server 2005 R2 hosts.

Virtual hard disks are stored in the virtual machine configuration file by absolute and relative paths to the vmc file. This arrangement provides Virtual Server 2005 R2 file portability, allowing it to find VHD files moved to other hosts with a different drive or path location. The relative path is used to prevent collisions if you made a copy on the same server.

Virtual network configuration files (.vnc) consist of a virtual network name, a bound physical adapter, and the configuration of the virtual Dynamic Host Protocol (DHCP) server. Virtual network names must be unique on a single host. Each virtual machine can have up to four virtual network adapters and be attached to four different virtual networks. The partnerships between virtual network adapters and virtual networks are stored in the virtual machine configuration file.

How It Works: Mapping a Virtual Network Adapter to a Physical Adapter

Mapping a virtual network adapter to a virtual network and then to a physical network adapter involves three files: the virtual machines .vmc, the virtual networks .vnc, and the options.xml host configuration file.

The .vmc file has an entry for each network adapter that specifies the *ID* of the *virtual_network* entry that is the virtual network it is attached to.

```
<ethernet_controller id="0">
         <ethernet_card_address type="bytes">0003FF1B6AD5</ethernet_card_address>
         <id type="integer">5</id>
         <virtual_network>
               <id type="bytes">00D67AACDFC2499DBD9222F7A0A29D54</id>
            <name type="string">Wireless</name>
         </virtual_network>
```

This maps to the .vnc file for the virtual network and the value for id. When these two values match, this is the virtual network that the virtual machine is attached to.

```
<settings>
        <gateway type="integer">22</gateway>
        <id type="bytes">00D67AACDFC2499DBD9222F7A0A29D54</id>
```

The options.xml file contains the binding to the physical network adapter using the gateway value of the .vnc file which maps to the id property value of the virtual_gateway entry.

```
<virtual_gateway id="7">
            <adapter type="string">\DosDevices\VPCNetS2_{CA746289-F2E6-405A-B7C2-
E2595ACA750A}</adapter>
          <id type="integer">22</id>
          <name type="string">Intel(R) PRO/Wireless 3945ABG Network Connection #2</name>
          <type type="integer">2</type>
     </virtual_gateway>
```

When you move the VNC from one machine to the other, only when the Virtual_gateway id matches between servers will it map properly to the physical adapter. It might be possible to have identical IDs between servers, but connected to different physical networks, so it is always better to reattach the VNC to the desired physical network adapter to be sure it is connected to the adapter you intended.

Best Practices You should establish naming standards for virtual machine configuration files as well as the computer name of the virtual machine. Virtual machine computer names should use the company naming standard for servers. Virtual machine configuration filenames should either match the virtual machine computer name or provide a way to group the machines in the user interface while including the virtual machine computer name.

For example, the company naming standard might be a three-letter location name followed by a server role designator, followed by a unique numeric value such as the following name:

HOUFS01

Using the standard three letter airport code designators will provide a preexisting recognized standard. The corresponding virtual machine name could be one of the following:

HOUFS01
F&P – HOUFS01

Using F&P in the beginning groups all file and print servers together in the Virtual Server 2005 R2 Administration Website user interface.

Best Practices You should establish virtual network naming standard to indicate the type of network attached: INTRANET, INTERNET, or TEST1. You should use a generic name that applies across multiple Virtual Server 2005 R2 hosts in a server farm. Refrain from using the network's address, such as 10.10.10.0, for virtual network names. Using common virtual network names throughout the server farm allows you to migrate a virtual machine between hosts without having to reset the virtual network connection.

Best Practices You should establish a virtual hard drive naming standard that allows you to quickly determine the computer name, drive type, and the drive number. The standard you choose should be well documented and followed to allow proper asset tracking.

Sample VHD Naming Standard

A sample VHD naming standard includes computer name, drive type, and drive number combined together to form a name like the following one:

```
ComputerName-Drivetype-drivenumber.vhd
```

The following table summarizes VHD naming standard components.

Naming standard component	Description
Computer Name	Virtual machine computer name
Driver type	I = IDE disk S = SCSI disk ID = IDE Differencing disk SD = SCSI Differencing disk
Drive number	VHD drive number for multiple VHD drives attached to a single machine

Using this standard, a virtual machine called HOUFS01 with two SCSI disks would produce the following:

```
HOUFS01-S-01.vhd – Disk 1
HOUFS01-S-02.vhd – Disk 2
```

Library of Virtual Machines

Provisioning a virtual machine in Virtual Server 2005 R2 is as simple as copying a set of files that combine to give virtual machines an identity. A library of virtual machines could include base machines with only the operating system installed, specific types of pre-installed application servers, and special-purpose virtual machines that have unattended installations of applications scripted to launch on boot and complete the installation.

Challenges to creating and maintaining a library of virtual machines include issues such as sysprepping images, minimizing provisioning time, managing updatess, and maintaining an authoritative source and replication system for distributing virtual machines.

Best Practices You should install and run sysprep on any virtual machine that will be added to the virtual machine library. While you are not limited to the number of times you can run sysprep on a machine, you are limited to the number of times that you can execute sysprep and reset product activation. That limit is three times. If you are going to sysprep a machine on a regular basis, you should not reset activation. Refer to the "Additional Resources" section of this chapter for more information about sysprep limitations.

Best Practices You should use dynamically expanding disks rather than fixed virtual hard disks to minimize the size of the virtual machines in the library. Doing so will dramatically reduce the amount of traffic transferred and reduce the load on your network.

You should automate the process of updating machines in the virtual machine library. Currently, there is no way to offline update a Windows operating system. Managing updates requires a script that automates the process or a procedure that describes the manual processes. An automated script requires the following steps:

1. Provision the virtual machines to a host machine.
2. Register the new virtual machine.
3. Power on the virtual machine.
4. Silently install all updates.
5. Power down the virtual machine.
6. Unregister the virtual machine.
7. Copy back the patched image to the library.

System Backup

Virtual Server 2005 R2 SP1 provides a new Volume Shadow Copy Service (VSS) writer. VSS writers are software interfaces included in applications and services that help provide consistent backups through the Volume Shadow Copy Service. The Virtual Server 2005 R2 SP1 writer responds to signals provided by the Volume Shadow Copy Service interface to allow the host and virtual machines to prepare their data stores for shadow copy creation by flushing all pending writes and to ensure that no writes occur on the volume while the shadow copy is being created. The VSS writer allows host and virtual machine backups to be performed from the host while the virtual machine is running. Without a VSS writer available, you would have to load a backup agent in every virtual machine, save the state, or shut down every virtual machine to ensure that memory and disk buffers are flushed to disk so that no data is lost.

The Virtual Server 2005 R2 SP1 VSS writer fulfills only half of the requirement. The backup application must implement support for the writer and have the ability to query the writer interfaces before it starts to back up the system. Refer to Chapter 17, "Managing a Virtual Server Infrastructure," for a detailed discussion of Virtual Server backup and the VSS writer.

Important Because Windows Server 2003 SP1 and R2 versions were released before Virtual Server 2005 R2 SP1, Windows Server 2003 SP1 and R2 versions of NTBackup are not aware of the Virtual Server 2005 R2 SP1 VSS writer interface. Therefore, NTBackup will not properly signal Virtual Server or virtual machines to quiesce all disk and memory buffers before trying to back up the files.

Best Practices You should purchase a backup application that is aware of the Virtual Server 2005 R2 SP1 VSS writer to perform backups on Virtual Server 2005 R2 SP1 hosts. This will allow you to minimize the effort and load associated with performing backups of virtual machines.

Summary

This chapter covered best practices to address common configuration, performance, and operational issues associated with deployments of Virtual Server 2005 R2. You can avoid configuration issues by modifying the default virtual machine configuration folder, adding custom search paths for easy selection of files in the Administration Website user interface, enabling VMRC, and selecting configuration options to provide a secure remote virtual machine management solution.

Host performance issues can be avoided by selecting appropriate memory configurations, enabling full acceleration for your graphics display adapter, selecting and correctly configuring the right network adapters, and purchasing a SAN with high-RPM SATA or SAS hard disks and iSCSI support. You can avoid virtual machine performance issues by following best practices for your host hardware configuration, using proper resource allocation settings, improving your display graphics performance by configuring for performance and not visual effects, installing virtual machine additions, and using fixed-size SCSI virtual hard drives.

Finally, you can keep operational headaches to a minimum by establishing naming standards, establishing a library of sysprep virtual machines, and using the new Virtual Server 2005 R2 SP1 VSS writer to obtain the most flexible and best-performing backups of host and virtual machines.

Additional Resources

The following resources contain additional information related to this chapter:

- Knowledge Base Article 830958, "Summary of the limitations of the System Preparation tool," at *http://support.microsoft.com/kb/830958/*
- White paper, "How Sysprep Works," at *http://technet2.microsoft.com/WindowsVista/en/library/fd2f79c9-3049-4b8c-bcfd-4e6dc5771ace1033.mspx?mfr=true*
- Knowledge Base Article 903748, "Virtual Server 2005 performance tips," at *http://support.microsoft.com/kb/903748/*
- Knowledge Base Article 925477, "Event IDs 1100, 1101, and 1102 are logged every time that the Virtual Server service starts in Virtual Server 2005 R2," at *http://support.microsoft.com/kb/925477/*
- White paper, "How Volume Shadow Copy Service Works," at *http://technet2.microsoft.com/WindowsServer/en/Library/2b0d2457-b7d8-42c3-b6c9-59c145b7765f1033.mspx?mfr=true*
- White paper, "Virtual Hard Disk Image Format Specification," at *http://www.microsoft.com/windowsserversystem/virtualserver/techinfo/vhdspec.mspx*
- White paper, "Using iSCSI with Virtual Server 2005," at *http://www.microsoft.com/downloads/details.aspx?FamilyID=d112aa63-a51e-4722-a41b-98b3ab3700a3&displaylang=en*
- White paper, "Application Software Considerations for NUMA-Based Systems," at *http://www.microsoft.com/whdc/system/platform/server/datacenter/numa_isv.mspx*

Chapter 10

Virtual Machine Migration Process

In this chapter:

This chapter focuses on the physical-to-virtual (P2V) migration process using the Virtual Server Migration Toolkit (VSMT), a free downloadable software tool used with Microsoft Virtual Server 2005 Release 2 (R2) to convert physical workloads into virtual machines (VMs). You will learn how to determine which workloads are good candidates for migration to a virtual machine and discover important factors to consider when defining workload resource requirements. The VSMT requirements, features, and deployment procedures are presented in detail, followed by step-by-step instructions to perform a physical to virtual machine migration. Additionally, the sequence to complete a virtual-to-virtual (V2V) machine migration is described.

Whereas VSMT is a viable tool to use for personal and small test and development environments where only a select number of P2V migrations must be accomplished and budget is limited, more robust and automatable tools are required for larger scale departmental, branch office, and data center environments. Microsoft System Center Virtual Machine Manager (VMM) is an enterprise-level application that can perform individual wizard-based P2V migrations or PowerShell-based scripted migrations. If you are interested in learning about VMM, you should review Chapter 19, "System Center Virtual Machine Manager 2007." There are also Independent Software Vendor (ISV) applications that support physical to virtual workload migrations, and these are covered in Chapter 20, "Additional Management Tools."

Assessing Physical Workload Virtualization Potential

The first step in the process to virtualize a physical workload is the assessment of its virtualization potential. The virtualization potential is determined by considering two major categories: workload requirements and workload limitations. The workload requirements are

defined by the physical memory, processor, network, and storage resources needed to achieve the required level of performance. The workload limitations include specific hardware or operational dependencies that could prevent workload execution in a constrained virtual machine environment. This section focuses on the assessment for a single workload. In Chapter 14, "Virtualization Project: Assessment Phase," the concept is extended to encompass workloads on an enterprise scale.

Defining the Workload Memory Requirement

To define the workload memory requirement for a virtual machine, you must identify peak memory usage on the physical system. The information should be distilled from performance data captured over a sufficiently long period of time to reflect an accurate workload memory usage profile. In computing environments that operate at a fairly constant level, data collection over a one- to two-week period might be sufficient. In other environments that experience regular periodic activity spikes (monthly, bi-monthly, and so on), data collection over a two- to four-week period might be necessary. Longer data collection periods might be required to capture activity spikes, if there are seasonal or other parameters that drive more irregular fluctuations.

Using the peak memory usage as the basis to calculate the required virtual machine memory allocation ensures that performance under peak load can be sustained. In fact, virtual machine memory allocation must also account for a 32-MB virtualization overhead that is a result of video random access memory (VRAM) emulation and code cache of recently translated nonvirtualizable instructions. Therefore, virtual machine memory allocation is calculated using the following formula:

VM Memory = Workload Peak Memory Usage + 32 MB

The Workload Peak Memory Usage is the value that you should allocate when you create a virtual machine. This value actually defines the maximum amount of memory that the virtual machine can use while it is running. If sufficient physical memory is not available during virtual machine start-up, an error is logged in the Virtual Server 2005 R2 event log and the virtual machine cannot start. Once a virtual machine is started, it remains loaded in memory until it is shut down.

Important If the virtual machine memory allocation calculation yields a result greater than 3.6 GB, you should perform a thorough review to determine if this peak value is sustained and disqualifies the workload or whether the peak value is of short enough span to qualify the workload as a viable virtualization candidate. Virtual Server 2005 R2 limits maximum memory allocation to 3.6 GB per virtual machine.

Once you have defined the virtual machine memory allocation requirement, you must determine the total amount of memory needed for the physical server host. Because Virtual Server 2005 R2 runs as an application above the host operating system, you must also consider the

Virtual Server host operating system memory requirements in addition to those of the virtual machine. Consequently, the total memory specification for the physical server is calculated as follows:

Server Memory = [Host Memory + VM Memory] × 1.25

Best Practices At minimum, you should add 25 percent to the server memory calculation for capacity planning. It is important for you to tune the percentage based on specific growth projections. Nonetheless, this approach provides a buffer to manage virtual machine memory growth requirements and handle additional virtual machines. For example, if a Microsoft Windows Server 2003 R2 host server running Virtual Server 2005 R2 requires 1 GB of memory and the virtual machine allocation was calculated as 3 GB, the formula yields the following:

Server Memory (rounded up to even number) = [1 GB (Host) + 3 GB (VM) + 32 MB (Overhead)] ×1.25

Server Memory (rounded up to even number) = 6 GB

Defining the Workload Processor Requirement

There are two factors to take into account when defining the workload processor requirement for a virtual machine: processor scaling and peak processor utilization. Understanding the processor scaling requirements for a specific workload is crucial to defining the workload virtualization potential. Although Virtual Server 2005 R2 can scale across multiple processors, a virtual machine can be allocated a maximum of only one processor core. Hence, a workload with symmetric multiprocessing (SMP) requirements might not be a good candidate for virtualization in a production environment. However, it might be acceptable to virtualize the workload for a test or training environment where performance is not the primary driver or the required performance can be achieved when running on a single, more powerful processor core.

The maximum sustained processor utilization is used to define the virtual machine processor allocation requirement. Maximum sustained processor utilization should be captured in the same set of performance data as the peak memory usage. Use the following formula to calculate the virtual machine processor requirement:

Processor Requirement = number of CPU Cores × CPU Speed × Utilization (maximum sustained)

For example, using a physical server with two single-core 2-GHz processors and a maximum sustained utilization of 10 percent, the formula yields:

Processor Requirement = 2 × 2000 MHz × 10% = 400 MHz

Caution This calculation assumes that the source and target processor architectures are similar enough to provide a valid processor performance comparison. If this is not the case, you need to include a performance factor in the calculation that corrects for the processor performance differences. You should also consider using a tool like System Center Virtual Machine Manager or another third-party tool that considers processor differences when determining virtual machine processor requirements.

Once the virtual machine processor requirement is known, you can determine the virtual machine CPU resource allocation settings to configure in Virtual Server 2005 R2. You should adjust these settings in anticipation of hosting additional virtual machines on the Virtual Server host. For example, if the Virtual Server 2005 R2 physical server includes two single-core processors running at 3.0 GHz, the server processor capacity is as follows:

Server Processor Capacity = 2 × 3000 MHz = 6000 MHz = 6GHz

Of course, processor capacity for the host operating system must be taken into account. Consider reserving at least 25 percent of the server processor capacity (or at least a single processor core, whichever is less) to determine the processor capacity available for allocation to virtual machines:

Available Processor Capacity = Server Processor Capacity × 0.75

You should fine-tune the reserved processor capacity if you intend to run other applications on the host operating system in addition to Virtual Server 2005 R2.

Best Practices The general recommendation is to dedicate a physical server as a Virtual Server host and to not run additional applications. There are scenarios, such as in branch offices, where only a single server can be deployed and must support multiple applications. However, you should only deploy this configuration in such instances and not as a broad virtualization solution.

For the dual-processor server with 6 GHz of processor capacity and a 25 percent host operating system processor capacity reservation, the available processor capacity to allocate to virtual machines is as follows:

Available Processor Capacity = 6000 MHz × 0.75 = 4500 MHz = 4.5 GHz

There is now sufficient information to define the virtual machine processor resource allocation relative weight, reserved capacity, and maximum capacity settings. Table 10-1 lists the basic definitions for each of these parameters. Chapter 2, "Virtual Server 2005 R2 SP1 Product Overview," contains more detailed information on the processor resource allocation settings

available in Virtual Server 2005 R2. Chapter 15 contains in-depth configuration guidance on setting these parameters in a multiple workload environment.

Table 10-1 CPU Resource Allocation Parameter Definitions

Parameter	Description
Relative Weight	A value used to determine additional processor resource allocation for a virtual machine compared to all other virtual machines in execution. By default, the relative weight is set to a value of 100, making all virtual machine resource requirements equal to each other.
Reserved Capacity (% of one CPU)	A value used to define the capacity of a single processor reserved for a virtual machine. The processor capacity allocated to the virtual machine is never less than this value.
Maximum Capacity (% of one CPU)	The maximum processor capacity that can be used by a virtual machine.

Continuing with the example of the single workload requiring a 400-MHz processor peak utilization and available processor capacity of 4.5 GHz, the CPU resource allocation settings are as follows:

Relative Weight = 100 (default setting)

Reserved Capacity (rounded up) = 4500 MHz / 400 MHz = 12 percent

Maximum Capacity = 100 percent (default setting)

There is no need to modify the default settings for relative weight and maximum capacity in the case of a single virtual machine. These settings should be revised based on workload priorities if additional virtual machines are hosted on the Virtual Server 2005 R2 machine.

Caution If you allocate processor resources that exceed available processor capacity, Virtual Server 2005 R2 will not turn on a virtual machine that would result in processor capacity overallocation. An error with Event ID 1042, indicating an unexpected error occurred, will be recorded in the Virtual Server application log.

Defining the Workload Network Requirement

The workload network requirement is another essential component in the identification of virtual machine resource needs. Analogous to the memory and processor requirements, the virtual machine network requirement is based on peak network utilization data captured from the workload executing on the physical server. This data is fundamental to determining whether the virtual machine requires one or more dedicated network interface cards (NICs), or if it can achieve desired performance levels using a shared network interface card.

In the case of a single virtual machine, if the workload on the physical server requires one or more dedicated network interface cards, you can implement the same configuration for the virtual machine. Depending on the fine points of the configuration, one or more virtual networks should be defined and connected to the appropriate network interface card to provide the required connectivity.

Important As a general rule, use a dedicated network interface card for the host operating system. This will ensure consistent communication with Virtual Server 2005 R2 and other applications installed directly on the host operating system. Also, unbind the Virtual Machine Network Service from the network interface card dedicated to the host to prevent any association to a virtual network within Virtual Server 2005 R2.

If multiple workloads without dedicated network interface card requirements will be hosted in virtual machines, use the following formula to determine the total network bandwidth utilization:

Total Network Requirement = SUM (NIC Speed × Peak Network Utilization)

As indicated, the total network requirement is simply based on the sum of the peak network bandwidth utilization of each workload. For example, consider four workloads running on physical servers configured with 100-Mb-per-second (Mb/s) network interface cards, and peak network utilization of 50 percent. Using the formula, the total network requirement is as follows:

Total Network Requirement = 4 × (100 Mb/s × 0.5) = 200 Mb/s

The result indicates that the combined virtual machine network requirement for the four workloads can be met using a single gigabit network interface card. Because network interface cards do not operate at 100 percent of capacity, assuming 75 percent network interface card efficiency, the remaining network capacity is as follows:

Remaining Network Capacity = (1000 Mb/s × 0.75) − 200 Mb/s = 550 Mb/s

Note If needed, use the Microsoft Loopback Network Adapter to enable connectivity between the Virtual Server 2005 R2 host and virtual machines. This will create a purely internal, isolated network that does not require configuration of a physical network interface card. Ensure that only the Virtual Machine Network Service is bound to the Loopback Network Adapter to dedicate it to Virtual Server networking. For further details, read the Microsoft Loopback Network Adapter configuration section in Chapter 4, "Installing Virtual Server 2005 R2 SP1."

As new workloads are hosted on the Virtual Server 2005 R2 machine, you should consistently review each workload's network requirement to determine whether there is sufficient bandwidth capacity provided by existing network interface cards.

Defining the Workload Storage Requirements

Defining the virtual machine workload storage requirement depends on the specification of storage capacity and performance. To properly configure and size the storage capacity, a number of aspects need to be considered besides the physical disk space profile. The workload performance requirement determines whether shared or dedicated storage configuration is needed to attain disk throughput levels.

Virtual machine storage capacity planning must account for additional disk space to store a Save State file coupled with the disk space needed for differencing and undo disks, if they are to be used in conjunction with the virtual machine. The Save State file (.vsv) size is directly dependent on the virtual machine memory allocation. For example, if a virtual machine has a 3-GB memory allocation, the Save State file size allocation will be 3 GB. In actuality, Virtual Server compresses the virtual machine memory content prior to saving it to the .vsv file; therefore, the size of the data saved to the .vsv file should always be smaller than the virtual machine memory allocation.

Note In Virtual Server 2005 R2 SP1, a blank save state file is created when you start a virtual machine. The file size is based on the virtual machine memory allocation. The file is deleted when the virtual machine is turned off. This feature prevents data loss in a scenario where a virtual machine runs out of space on the physical hard disk where its VHD is located. Basically, Virtual Server 2005 R2 SP1 pre-allocates a large enough save state file for each running VM such that it can perform a save state for each affected running virtual machine.

Defining additional disk space to account for differencing and undo disks is a little more complex. Differencing disks and undo disks are special-purpose dynamically expanding virtual hard disks that allow virtual machine state changes to be saved in files that are separate from a base virtual hard disk. Differencing disks and undo disks both have the ability to grow as large as the base virtual hard disk. If a differencing or undo disk attempts to expand and causes the underlying physical drive to run out of disk space, Virtual Server 2005 R2 will suspend the virtual machine and place it in a saved state. Hence, to avoid virtual machine downtime, make sure to size storage capacity taking into account the size of each differencing and undo disk that will be used with the virtual machine.

Allowing for these factors, the virtual machine workload storage capacity requirement is defined as the aggregate of the following:

- Disk space used by the virtual machine VHDs on the physical server environment

- Disk space to be used by a Save State file, equivalent to the virtual machine memory allocation
- Disk space to be used by all differencing disks and undo disks associated with the virtual machine
- Disk space overhead no less than 25 percent of the total to provide additional storage and defragmentation capacity

In conjunction with storage capacity, you must also consider the workload storage performance requirement. The peak disk utilization for the physical workload and throughput attributes for the physical storage system are the key characteristics to consider when designing the physical storage environment to host virtual hard disks. Keep the following items in mind throughout the process:

- Use a fast access disk subsystem or storage area network (SAN).
- Use RAID 1+ 0 for the best disk performance or RAID 5 as an alternative in terms to support virtual hard disk storage.
- Dedicate disks and I/O channels for applications with very high throughput requirements.
- Dedicate disks for the host operating system and page file.
- Perform regular disk defragmentation.

As you add new virtual machines to Virtual Server 2005 R2, you must reassess whether the storage configuration and performance is sufficient to host additional workloads. If it is not, determine whether additional or dedicated disk resources are required and configure the storage environment to meet the new requirements.

Important To achieve the highest performance within the virtual machine, use fixed-size virtual hard disks connected to virtual SCSI adapters. Fixed-size virtual hard disks support up to 2 terabytes of data and will have less fragmentation than dynamically expanding disks. The SCSI protocol allows for multiple simultaneous operations, leading to higher throughput than IDE-connected virtual hard disks.

Defining the Workload Hardware Limitations

Because virtual machines execute within a constrained emulated hardware environment, some physical server workloads are precluded from a physical to virtual machine migration. In particular, disqualify any workloads that require the following items:

- USB devices (other than a keyboard and mouse)
- IEEE 1394 devices
- Non-Ethernet network interface cards

- Specialized SCSI adapters
- Specialized video or audio adapters
- Hardware dongles

The list is not exhaustive. However, it is evident that if a workload requires a specialized hardware device, it is not a suitable candidate for migration to Virtual Server 2005 R2.

Defining the Workload Operational Limitations

Finally, you must also consider any workload operational limitations in the assessment of a physical workload's suitability for migration to a virtual machine. For example, the following Microsoft server applications are not supported in a Virtual Server 2005 R2 production environment:

- Microsoft Speech Server
- Microsoft ISA Server 2000
- Microsoft ISA Server 2004
- Microsoft SharePoint Portal Server 2003
- Microsoft Identity Integration Server 2003
- Microsoft Identity Integration Feature Pack

If an application vendor does not support deployment of an application in a Virtual Server 2005 R2 production environment, it is not recommended that you do so. However, you can still leverage Virtual Server 2005 R2 to deploy the application in a testing or training environment.

Understanding the Physical to Virtual Workload Migration Process

The migration of a physical workload to a virtual machine consists of the three main phases described in Table 10-2. These phases are common to most migration tools available on the market, including the free, downloadable VSMT mentioned earlier in the chapter.

Table 10-2 Physical-to-Virtual Workload Migration Phases

Migration phase	Description
System Preparation	In the first phase, the source system is prepared for the migration process. If needed, the target system configuration is modified to comply with migration tool prerequisites and settings.
Workload Image Capture	In the second phase, migration tools collect source system configuration data, validate that the source system configuration is suitable for migration, and complete the workload image capture.
Virtual Machine Creation and Deployment	In the last phase, the migration tool creates, configures, and deploys a new virtual machine using the captured workload image.

The details of each phase presented in this section describe the process specifically implemented by VSMT to perform a physical-to-virtual workload migration. VSMT is a set of tools and customizable scripts used to collectively complete the migration process.

To use VSMT, you must be proficient with the Dynamic Host Configuration Protocol (DHCP), Pre-boot Execution Environment (PXE), and Windows Server 2003 Automated Deployment Services (ADS). If you are unfamiliar with one or more of these technologies, training material suggestions are provided at the end of this chapter in the "Additional Resources" section.

System Preparation Phase

Before using VSMT to perform a workload migration, the source system configuration must be evaluated to ensure compliance with the prerequisites listed in Table 10-3. These requirements specify not only the infrastructure protocols that the source system must support, but also characteristics—such as the operating system and file system type—that are driven by the boundaries of applicability of ADS and VSMT.

Table 10-3 Virtual Server Migration Toolkit Prerequisites

Prerequisite	Description
Pre-boot Execution Environment	The source system primary network interface card must support the PXE 0.99c protocol and allow a PXE boot from ROM or using a Remote Boot Disk Generator (RBFG) disk.
Dynamic Host Configuration Protocol	The source system must be able to obtain a network address and network configuration parameters from a DHCP server.

Table 10-3 Virtual Server Migration Toolkit Prerequisites

Prerequisite	Description
Hardware Abstraction Layer (HAL)	The source system must use one of the following hardware abstraction layer types: ■ Advanced Configuration and Power Interface (ACPI) PC - ACPI, PIC ■ ACPI Uniprocessor PC ■ ACPI Multiprocessor PC ■ Standard PC ■ MPS Uniprocessor PC - APIC, Non-ACPI ■ MPS Multiprocessor PC - APIC, Non-ACPI
Operating System	The source system must be running one of the following operating systems: ■ Microsoft Window NT Server 4.0, Service Pack 6a ■ Microsoft Windows 2000 Server, Service Pack 4 ■ Microsoft Windows 2000 Advanced Server, Service Pack 4 ■ Microsoft Windows Server 2003, Standard Edition ■ Microsoft Windows Server 2003, Enterprise Edition
Memory	The source system must have a minimum of 96 MB of physical memory.
Network Adapter	The MAC address of the primary network interface card that will be used during the migration must be identified. VSMT requires specification of the network interface card MAC address when multiple devices are present.
Disk Type	The source system must use basic disks. Dynamic disks cannot be migrated using VSMT.
File System	The source system drives must use NTFS. File allocation table (FAT) partitions cannot be migrated using VSMT.
Storage Area Network (SAN)	The source system must not have any SAN connections to migrate. If any such connections exist, the data must be copied to a virtual hard disk using either a backup and restore procedure or standard file copy process.
Windows Management Instrumentation (WMI)	The source system must have Windows Management Instrumentation installed and functional.
Security Account	An account with local Administrator rights on the source system must be used to execute the various VSMT utilities and scripts.

If the source system boot partition profile does not conform to the requirements, the discrepancies must be fixed prior to starting the actual migration process. Otherwise, the migration procedure will not be successful. Data partitions can be migrated separately to individual VHD files using a file copy or disk imaging tool.

Workload Image Capture Phase

The next phase of the migration process consists of several tasks that conclude with the workload image capture. VSMT uses a set of tools and scripts to complete this objective. Following are the four key actions taken during this phase of the migration process:

1. Inventory source system configuration
2. Validate source system configuration
3. Generate migration scripts
4. Capture source system image

Inventory Source System Configuration

The first step in this phase is accomplished by running the GatherHW.exe utility, included in VSMT, on the source system. GatherHW.exe conducts an inventory of the source system configuration and stores it in an XML file. GatherHW.exe collects the following type of information:

- Operating system configuration (version, language, service packs, HAL, and so on)
- General system configuration (BIOS, processors, memory, and so on)
- Storage configuration (controllers, physical disks, logical drives, and so on)
- Network configuration (adapters, TCP/IP settings, MAC address, and so on)
- Secondary hardware configuration (video, audio, serial port, CDROM, and so on)
- Software configuration (services, drivers, updates, and so on)

The GatherHW.exe utility uses the Windows Management Instrumentation interface to collect system configuration information.

Validate Source System Configuration

The second step in the workload capture phase uses VMScript, which is a VSMT script, to analyze the XML configuration file created by the GatherHW.exe utility and report on issues that could cause a migration failure. In fact, VMScript is a dual-purpose tool used not only to validate the source system configuration information prior to migration, but also to generate necessary migration scripts and files, as you will see in the next step.

In this step, VMScript is invoked to parse the XML file, determine whether any component or setting incompatibilities exist, and create a report similar to the following example:

```
Microsoft Virtual Server Migration Toolkit - VmScript Tool ver.5.2.5149.0
Copyright (C) 2004 Microsoft Corporation. All rights reserved.
Parsing System Configuration
        Name:         CONTOSO-ADS
        Memory:       1015MB
        Processors:   1
        HAL type:     acpipic_up
        OS Version:    5.2.3790 Service Pack 1
Parsing Network Configuration
        Network Card[0]
                MACAddress:  000AE45A7D1B
                DHCPEnabled:  True
                PrimaryNic : True
Parsing Storage Controller Configuration
        Controller ide[0]: PCI\VEN_8025&REV_03\3&61AAA01&0&F9
Parsing Logical Drive Configuration
        Found 1 logical disk drives
                Logical Drive[C:]
                        Size:                    12584644608
                        Hosts Windows Partition: True
Parsing Hard Disk Configuration
        Found 1 disk drives
        Disk Drive[0]: (\\.\PHYSICALDRIVE0)
                Size:      100027630080
                Partitions found: 1
                Partition[1]
                        Primary:                 True
                        Bootable:                True
                        Hosts Windows Partition: True
                        Able to Capture:         True
                        Extended Partition:      False
                        BootIni:                 True
                        Logical Drives:          C:
Parsing CDROM Configuration
        Found 1 cdrom drives
        CDROM Drive[0]: (IDE\CDROMPIONEER_DVD-RW_DVR-K13RA02020202)
Parsing Services Configuration
        Found 88 services
Parsing Drivers Configuration
        Found 174 drivers
Parsing Auto Run Programs Configuration
        Found 2 auto run programs
Parsing System File information
        Found 11 system files
Parsing Hotfix information
        Found 56 hotfixes
Parsing MountedDevices information
        Found 6 mounted device entries
Mapping Storage Devices
Using Windows Partition: \device\harddisk0\partition1 Disk:0 Partition:1
Using MAC[1]=000AE45A7D1B for PXE (Admin)
Checking configuration for incompatibilities.
No incompatibilities found.
Success.
```

VMScript also checks for problematic services or drivers, auto-run programs, key system files, and missing patches. The script then determines the primary operating system partition and MAC address of the network interface card that it should use for the workload image capture.

Direct from the Source: Identify and Load Missing System Files, Service Packs, and Updates

In the course of the source system configuration validation, VMScript reports whether any required system files are missing. The report includes the name of operating system files, service packs, or updates that contain system files that VSMT will need to perform a successful migration.VMScript uses an XML-based file, PatchFiles.xml, that is included with VSMT to determine which files are missing.

For English-language versions of supported operating systems, only files with updates and service packs available prior to the VSMT release are included with the toolkit. Equivalent files for non-English operating systems are not included by default. If you perform an operating system migration that requires an update or system file that was not included with VSMT, you must load the system files prior to initiating the migration.

To update the VSMT system file cache, use the Vmpatch.exe utility that comes with the toolkit. Vmpatch.exe loads required system files from the operating system driver cache or any folder where the source files are stored.

Because Vmpatch.exe is unable to directly copy service pack or updated binary files into the file system cache, begin by extracting the service pack or update file from the binaries and placing them into a folder. Then use Vmpatch.exe to load the required files into the VSMT system file cache.

Once all missing files have been loaded, you should run VMScript again to verify that you remedied all file issues and that no other incompatibilities exist. If the VMScript reports no further issues, you can proceed with generating migration scripts.

Eric Winner
Lead Program Manager, System Center Virtual Machine Manager

Generate Migration Scripts

Once VMScript has validated the source system configuration, the next step is to generate the scripts and files needed to capture the workload image and complete the migration. Table 10-4 lists the predefined scripts and task sequence files generated by VMScript based on the XML configuration file created by the GatherHW.exe utility.

Table 10-4 Migration Scripts and Task Sequence Files

Script/File	Description
*Source*_commonInit.cmd	Sets common environment variables.
*Source*_capture.cmd	Calls *Source*_commoninit.cmd to set common environment variables. Adds the source computer as a device in the ADS database. Initiates the ADS task sequences in capture-disk.xml to capture an image for each hard disk partition on the source system. Releases control of the device, and removes it from the ADS database when the capture is complete. Fixes certain system files on the captured images to make them compatible with the virtual machine environment.
*Source*_CreateVM.cmd	Creates a virtual machine on Virtual Server. Removes all network adapters from the virtual machine. Adds network adapters, the last one is the network adapter that will be used for PXE. Connects the Remote Installation Services (RIS) virtual floppy disk. Creates virtual hard disks, and attaches them to the virtual machine. Adds CD-ROM and DVD. Adds SCSI controllers, as required. Adds the virtual machine as a device in the ADS database. Creates a series of ADS actions to set a number of variables. Uses discovery to get information from the virtual machine. Opens the Virtual Server Administration Website.

Table 10-4 Migration Scripts and Task Sequence Files

Script/File	Description
*Source*_DeployVM.cmd	Calls *Source*_commoninit.cmd to set common environment variables. Connects the RIS boot floppy. Starts the virtual machine. Boots the virtual machine into the ADS Deployment Agent, runs the ADS deployment disk sequence in DeployVM.xml, and deploys the images to the virtual machine. Updates storage drivers. Runs the ADS task sequences, HAL.xml and Uniproc.xml, as needed to update the HAL and NTOSKRNL to single-processor versions compatible with the virtual machine environment. Runs the ADS service task sequence, *Source*_ServiceDriver.xml, to set the start state of devices and services in the virtual machine.
*Source*_PostDeploy.cmd	Resets attributes of the boot.ini file to System, Hidden, and Read-Only. For a source Windows NT 4.0 Server SP6a, the following tasks are also performed: ■ Runs fixsetup.cmd to update the Setup.log file in the winnt\repair directory to reflect that the operating system is running on a single-processor computer. ■ Service packs and hotfixes use the information in the Setup.log file to install the appropriate components.
*Source*_CleanupVM.cmd	Invokes only in the case of a failed migration attempt. Calls *Source*_Commoninit.cmd to set common environment variables. Stops running jobs, and turns off the virtual machine. Removes the virtual machine from Virtual Server. Releases control of the device in ADS. Removes the device from ADS. Deletes the virtual machine configuration file, as well as any virtual hard disk files associated with the virtual machine.

Table 10-4 Migration Scripts and Task Sequence Files

Script/File	Description
*Source*_captureDisk.xml	Boots the source system to the ADS Deployment Agent. Gets disk geometry (cylinders, heads, and sectors) for each disk. Captures an image for each partition. Shuts down the source system.
*Source*_DeployVM.xml	Obtains disk geometry (cylinders, heads, and sectors) for each physical hard disk. Initializes virtual hard disks. Creates disk partitions for the virtual hard disks. Obtains geometry for disk partitions. Deploys ADS images to the virtual machine.
*Source*_internalState.xml	Captures the state of internal hardware for each device.
*Source*_ServiceDriver.xml	Configures the starting state of services and devices in a virtual machine.

By default, the scripts are configured to create an unencrypted workload image. When migrating a physical system that stores sensitive or protected data, edit *Source*_captureDisk.xml and *Source*_DeployVM.xml and remove all instances of the following statement:

```
<parameter>-nonetencrypt</parameter>
```

Doing so will cause workload images to be encrypted when captured and deployed using VSMT.

Capture Source System Image

The last step in this phase is to capture the workload image from the source system. The process starts by executing the *Source*_capture.cmd script. This script invokes ADS, and by using the *Source*_capturedisk.xml sequence file, it completes four basic tasks.

The first task adds the source system to the device database controlled by ADS. Second, the source system is booted using PXE and ADS uploads the Deployment Agent to the source system. The Deployment Agent is a small-footprint, memory-resident operating system that provides an execution shell that can run additional commands to capture and deploy system images to ADS-controlled devices. The third task consists of retrieving source system disk information and capturing an image of each disk. Finally, once an image has been captured for each disk, ADS initiates a shutdown of the source system, releases control of it, and removes it from the device database.

Additionally, the attribute settings of specific system files in the captured images are modified to ensure compatibility with the virtual machine environment.

Note The time required for the image capture process varies, ranging anywhere from 0.5 to 1.5 GB per minute. For source systems with large disks, use a conservative transfer rate to estimate planned downtime and user impact as well as the number of concurrent migrations that can be supported by your network.

Virtual Machine Creation and Deployment

In the last phase of the migration process, a new virtual machine is created and then deployed after the source system disk images are restored to attached virtual hard disks. The process begins with the execution of the *Source*_CreateVM.cmd script to check the status of the target system in the ADS database. To perform the virtual machine creation tasks, the *Source*_CreateVM.cmd invokes the VMClient.exe utility from VSMT. VMClient.exe creates and configures virtual machines on Microsoft Virtual Server 2005 R2 through the Virtual Server Component Object Model (COM) interface.

VMClient uses a multistep procedure to create a virtual machine on Microsoft Virtual Server 2005 R2. First, VMClient constructs and registers a virtual machine configuration file (.vmc) to create a new virtual machine. When the new virtual machine is registered with Virtual Server, VMClient adds virtual network adaptors with corresponding source system MAC addresses to the new virtual machine and connects them to a pre-created virtual network. Finally, a Remote Installation Services (RIS) floppy disk image is assigned to the virtual machine, the virtual hard disks are created and initialized, and a virtual CD drive is attached to the virtual machine.

The virtual machine is created using the memory, disk size, network adapters, and MAC address information collected from the source system configuration file. By default, the processor allocation is 100 percent of a single CPU. Unless otherwise specified, virtual hard disks are created as fixed-size disks. Because the virtual hard disks are created sequentially, the disk initialization period can be quite long.

Important Modifications to the virtual machine creation options and resource allocations are made by updating the appropriate VMClient command lines in the *Source*_CreateVM.cmd script. For complete details on the VMClient.exe options and parameters, review the Microsoft Virtual Server 2005 Migration Toolkit help file, VSMT.chm, which can be found in %systemdrive%\Program Files\Microsoft VSMT\Help.

The *Source*_CreateVM.cmd script completes after adding the new virtual machine to the ADS database, ensuring it is ready for deployment.

Virtual machine deployment is controlled by the *Source*_DeployVM.cmd script and the task sequence file, *Source*_DeployVM.xml. The *Source*_DeployVM.cmd script invokes the VMClient utility to start the virtual machine from the RIS virtual floppy disk. The virtual machine

acquires an IP address, and PXE boots into the ADS Deployment Agent. Once the virtual machine is booted, source system disk images are restored sequentially to the virtual hard disks. After the image restore procedure completes, the hardware-dependent system files are swapped for virtual machine–compatible versions and the virtual machine is powered off. At this point, the workload migration from source system to virtual machine is complete.

Using Automated Deployment Services and the Virtual Server Migration Toolkit

In this section, you will learn how to install ADS and VSMT to perform a physical to virtual machine migration. A full installation of ADS is described, including all the tools, samples, and templates needed to manage devices, capture disk images, and deploy disk images. As described in the previous section, VSMT leverages ADS to capture source system disk images, create virtual machines, and deploy source system disk images to virtual machines.

The following procedures are based on the assumption that ADS, VSMT, and Microsoft Virtual Server 2005 R2 SP1 are installed on a single physical server, referred to as the *Controller server*. This is not a requirement, but it is recommended as the quickest way to deploy and familiarize yourself with the tools and migration steps using a small footprint test environment. You will also need a second physical machine running the Windows Server 2003 operating system to represent a source system workload that will be migrated to a virtual machine.

Installing Automated Deployment Services

ADS is a Windows Server 2003 add-on that is available as a free download from the Microsoft Web site. The installation is straightforward with minimal requirements, as shown in Table 10-5.

Table 10-5 Automated Deployment Services Prerequisites

Requirement	Specification
Operating System	Windows Server 2003, Enterprise Edition.
DHCP Server	Any existing DHCP server that can provide TCP/IP network configuration settings to devices on the same network as the ADS server. Alternatively, install DHCP on the ADS server.
Database	Access to an existing Microsoft SQL Server to host the managed device database. Alternatively, install the Microsoft SQL Server Desktop Engine using the Automated Deployment Services Setup Wizard.
Storage	Size the disk space allocated to store source system images based on the physical disks that will be imaged.

The ADS installation includes the Controller Service, Image Distribution Service, and Network Boot Services. Once the installation package is downloaded, run the self-extracting executable and ensure that all the files are successfully extracted and placed into a new directory. To complete a full installation of ADS, follow these steps:

1. On the Controller server, use Windows Explorer to navigate to the directory that contains the extracted Automated Deployment Services installation files.
2. To begin the installation, locate and double-click the ADSSetup.exe file.
3. In the Welcome To Microsoft Windows Server 2003 Automated Deployment Services dialog box, click Install Microsoft SQL Server Desktop Engine (MSDE) SP4 (Windows) to create the Automated Deployment Services device database.
4. Once MSDE is installed, click Install Automated Deployment Services to start the Automated Deployment Services Setup Wizard.
5. In the Welcome To The Automated Deployment Services Setup Wizard dialog box, click Next.
6. In the License Agreement dialog box, review the license agreement. If you agree to the terms of the license, click I Accept The Terms Of The License Agreement and then click Next.
7. In the Setup Type dialog box, select Full Installation and then click Next.
8. In the Installing PXE dialog box, click OK.
9. In the Setup Type dialog box, click Next.
10. In the Configure The ADS Controller dialog box, use the default settings and click Next.
11. In the Network Boot Service Settings dialog box, select Prompt For The Path When Required and then click Next.
12. In the Windows PE Repository dialog box, click Do Not Create A Windows PE Repository and then click Next.
13. In the Image Location dialog box, use the default path or type a new path in the Path To Folder box, and then click Next.
14. If ADS Setup detects more than one network adapter in your computer, it displays the Network Settings For ADS Services dialog box. In the Bind To This IP Address text box, specify the IP address to bind the services and click Next.
15. In the Installation Confirmation dialog box, click Install.
16. In the Installing ADS dialog box, a progress bar appears to indicate the status of the installation.
17. When the Completing The Automated Deployment Services Setup Wizard dialog appears, click Finish.

18. During the installation process, a certificate is created to authenticate devices that interface with Automated Deployment Services. After the installation is complete, create a shared folder and copy %systemdrive%\Program Files\Microsoft ADS\Certificate \adsroot.cer into the shared folder.
19. Using Windows Explorer, navigate to %systemdrive%\Program Files\Microsoft ADS \Samples\Sequences and double-click on create-templates.bat. This will install sample job templates that are available to run and test the services.

To verify that the ADS installation was successful, use the Microsoft Management Console (MMC) snap-in to check whether the services are in the Connected state as shown in Figure 10-1.

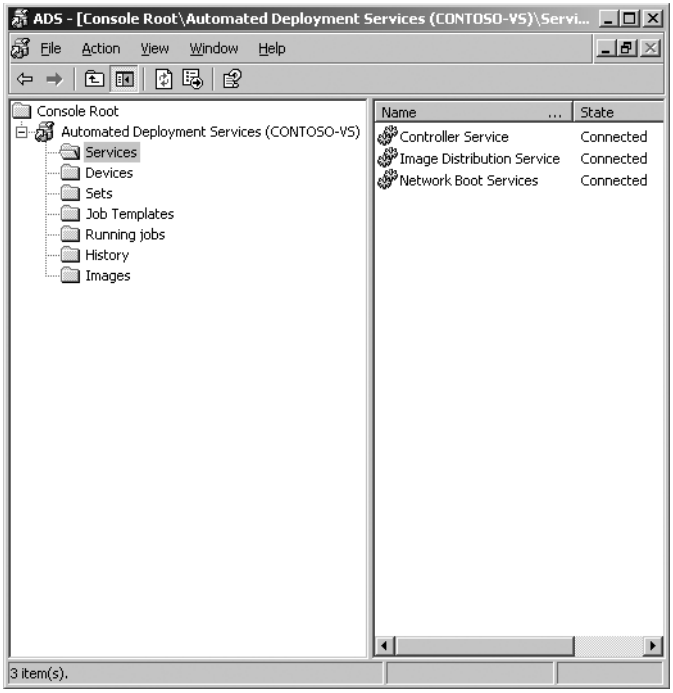

Figure 10-1 Automated Deployment Services connected state

To use the Automated Deployment Services MMC snap-in, follow these steps:

1. Click Start, click Run, in the Run dialog box, type **ads.msc**, and then click OK.
2. In the ADS-[Console-Root], click Automated Deployment Services in the left-hand pane to expand the tree structure, and then click the Services entry.

If all the service bindings were successful, the Controller Service, Image Distribution Service, and Network Boot Services states should display "Connected."

Installing the Virtual Server Migration Toolkit

VSMT is included in the Automated Deployment Services 1.1 installation package. Prior to installing the toolkit, ensure that you have already installed Microsoft Virtual Server 2005 R2 SP1 and ADS on the physical server.

To complete a full installation of VSMT, follow these steps:

1. On the Controller server, use Windows Explorer to navigate to the directory that contains the extracted Automated Deployment Services installation files.
2. To begin the installation, locate and double-click the ADSSetup.exe file.
3. In the Welcome To Microsoft Windows Server 2003 Automated Deployment Services dialog box, click Install Virtual Server Migration Toolkit.
4. In the Welcome To The Microsoft Virtual Server 2005 Migration Toolkit Setup Wizard dialog box, click Next.
5. In the License Agreement dialog box, review the license agreement. If you agree to the terms of the license, click I Accept The Terms Of The License Agreement and then click Next.
6. In the Setup Type dialog box, select Full Installation and then click Next.
7. In the Installation Confirmation dialog box, click Install.
8. In the Installing VSMT dialog box, a progress bar appears to indicate the status of the installation.
9. When the Completing The Microsoft Virtual Server 2005 Migration Toolkit Setup Wizard dialog box appears, click Finish.

At this time, you should also pre-create the default virtual network (VM0) that the *Source*_CreateVM.cmd script attaches to a new virtual machine. The virtual network is not created by default during the VSMT installation because the setup process does not assume that it is installed on the same physical system as Microsoft Virtual Server 2005 R2.

A script is provided with VSMT to automatically create the default virtual network. If the default virtual network does not exist, the virtual machine deployment will fail. To create the default virtual network using the script, follow these steps:

1. Using Windows Explorer, navigate to %systemdrive%\Program Files\Microsoft VSMT \Samples.
2. Locate and double-click the CreateVirtualNetwork.vbs file.
3. Open the Microsoft Virtual Server 2005 R2 Administration Website in your browser.
4. In the Virtual Networks pane, click Configure and verify that there is an entry for VM0 in the list of virtual networks.

Alternatively, you can execute the script by opening a command window and typing the following:

```
Cscript "%systemdrive%\Program Files\Microsoft VSMT\Samples\createvirtualnetwork.vbs"
```

Note You can also use a VMScript command-line option called /vsHostNet when generating the migration scripts to specify a different virtual network to use during the migration.

Performing a Physical to Virtual Machine Migration

Once the ADS and VSMT installations are completed, you are ready to begin the physical-to-virtual machine migration. The migration procedure consists of ten steps:

1. Preparing the source system.
2. Gathering the source system configuration information.
3. Validating the source system configuration information.
4. Generating the migration scripts.
5. Reviewing the migration scripts.
6. Loading drivers into ADS.
7. Capturing the source system disk images.
8. Creating the virtual machine.
9. Deploying the source system disk images to the virtual machine.
10. Completing the migration process.

To prevent any loss of data during the migration process, make a backup of the source system prior to starting the migration process. This step is particularly critical if you intend to migrate Windows NT 4.0 servers because the NTFS file system will be upgraded during the migration procedures.

Preparing the Source System

As part of the source system preparation, use the requirements list in Table 10-3 and Table 10-5 to ensure that the source system satisfies the conditions imposed by ADS and the VSMT for a successful migration. In addition, use the Chkdsk.exe utility to verify and resolve any disk errors, delete irrelevant or outdated files, and defragment the disks prior to the migration.

Note On a system running Windows NT Server 4.0, Service Pack 6a, you must install hotfix 872952 to ensure that the Chkdsk.exe utility still functions after the physical to virtual machine migration. Hotfix 872952 is available at *http://support.microsoft.com/kb/872952*.

If for any reason you intend to perform a migration from a source system configured with hardware drivers or services that are incompatible with the virtual machine environment, change the startup state to Disabled before starting the migration. Leaving incompatible drivers or services in an automatic startup state can cause the virtual machine to function improperly or fail to start.

Important If you use ADS to manage the source system, release control of the source system and delete the source system record prior to initiating the migration.

Gathering the Source System Configuration Information

When the system preparation is complete and the source system meets all the defined requirements, the next step is to run the GatherHW.exe tool from the VSMT. GatherHW.exe collects the source system information and creates an XML file that contains the system configuration data. Follow these steps to run GatherHW.exe on the source system:

1. Log on to the source system running Windows Server 2003.
2. Map a network drive to the root of the system drive on the Controller server.
3. Navigate to the Virtual Server Migration Toolkit installation folder, which is by default %systemdrive%\Program Files\Microsoft VSMT.
4. Copy GatherHW.exe to a directory on the source system.
5. Double-click GatherHW.exe on the source system to collect the configuration information.
6. GatherHW.exe creates an XML file with the name of the source system (*Source*.xml) in the directory from which GatherHW.exe was executed.
7. Copy *Source*.xml to the Controller server. If you followed the recommended procedure, Microsoft Virtual Server 2005 R2, VSMT, and ADS are installed on the Controller server.

Validating the Source System Configuration Information

After executing GatherHW.exe to collect the source system configuration information, you need to validate the data using the VMScript.exe utility. When VMScript.exe completes the configuration information analysis, it will indicate whether any errors or issues were encountered. Follow these steps to run VMScript.exe on the source system:

1. Log on to the Controller server and open a command window.
2. In the command window, change the directory to the Virtual Server Migration Toolkit installation folder, which by default is %systemdrive%\Program Files\Microsoft VSMT.

3. In the command window, start the VMScript execution by typing the following:

   ```
   VMScript.exe /hwvalidate /hwinfofile:"path\Source.xml"
   ```

   where *path**Source.xml* is the full path to the XML file.

Examine the VMScript output for any flagged issues, warnings, or errors. Correct any system discrepancies, and copy any missing system files, service packs, or hotfix files using VMPatch.exe before continuing to the next step.

Note For complete details on the VMPatch.exe options and parameters, review the Microsoft Virtual Server 2005 Migration Toolkit help file, VSMT.chm, located in %systemdrive%\Program Files\Microsoft VSMT\Help.

Generating the Migration Scripts

Once VMScript.exe has validated the source system configuration information, the next step is to execute VMScript.exe with a different set of options that generate the migration scripts that control disk image capture, virtual machine creation, and disk image deployment to the virtual machine. Follow these steps to generate the migration scripts using VMScript.exe:

1. Log on to the Controller server and open a command window.
2. In the command window, change the directory to the Virtual Server Migration Toolkit installation folder, which by default is %systemdrive%\Program Files\Microsoft VSMT.
3. In the command window, start the VMScript execution by typing the following text:

   ```
   VMScript /hwgeneratep2v /hwinfofile:"path\Source.xml" /name:vm_name /vmconfigpath:"vm path" /virtualDiskPath:"vm path" /hwdestvs:controller_server
   ```

   where *path**Source.xml* is the full path to the XML file, *vm_name* is the name to assign to the virtual machine, *vm path* is %systemdrive%\Program Files\Microsoft VSMT\VMs, and *controller_server* is the name of the Controller server.

Important By default, the migration scripts are configured to create fixed-size virtual hard disks. If the physical disks on the source system have an extensive amount of unallocated free space or you do not want to use fixed-size virtual hard disks, execute VMScript with the /virtualDiskDynamic option. This option directs VMScript to generate migration scripts that create dynamically expanding virtual hard disks. Forcing the migration scripts to create dynamically expanding virtual hard disks also reduces the total time to complete the migration by minimizing the virtual hard disk initialization process.

VMScript.exe generates the migration scripts in a subdirectory of %systemdrive%\Program Files\Microsoft VSMT\p2v. The subdirectory is given the same name assigned to the virtual machine. For example, if you provide *TestMigration* as the parameter to the VMScript /name

option, the migration scripts are created in %systemdrive%\Program Files\Microsoft VSMT\p2v\TestMigration. All the generated migration files are also prefixed with the name of the virtual machine. Before moving to the next step, verify that the VMScript.exe output indicates that the migration files were created successfully.

Reviewing the Migration Scripts

Once the migration scripts are generated, you should familiarize yourself with each script and XML task sequence file. If any problems arise during the remaining migration tasks, it will be more difficult to troubleshoot issues if you are unfamiliar with the contents and actions contained within the generated migration scripts and files.

Loading Drivers into Automated Deployment Services

Even if VMScript successfully validates the source system configuration information, you must determine whether the network interface card installed in the source system is directly supported by ADS. If you had to load external network interface card drivers when you installed the operating system on the source system, you will most likely have to copy the same driver files into the Automated Deployment Services file cache before you can proceed and capture the source system disk image.

Follow these steps to copy and process the network interface card drivers into the Automated Deployment Services file cache:

1. Log on to the Controller server.
2. Download the latest network interface card drivers for the source system to a temporary directory.
3. Copy the driver files into %systemdrive%\Program Files\Microsoft ADS\NBS \Repository\User\PreSystem.
4. Open a command window.
5. In the command window, type **net stop adsbuilder** and then press Enter.
6. In the command window, type **net start adsbuilder** and then press Enter.

When you copy the network interface card driver files into the Automated Deployment Services file cache, do not create any subdirectories or include Txtsetup.oem files.

Note For more details on the issues that you can encounter when ADS lacks network interface card drivers for the source system, review Microsoft Knowledge Base article 841550 at *http://support.microsoft.com/kb/841550*.

Capturing the Source System Disk Image

At this stage, you are ready to capture the source system disk images. The *Source*_Capture.cmd migration script executes and leverages ADS to capture each source system disk image sequentially.

Follow these steps to start the source system disk image capture process:

1. Log on to the Controller server and open a command window.
2. In the command window, change directory to the Virtual Server Migration Toolkit sub-directory where the generated migration files are stored.
3. In the command window, execute the *Source*_capture.cmd script.
4. When prompted, log on to the source system, restart it, and PXE boot it.

ADS takes control of the source system and boots it into the Deployment Agent to initiate the disk image capture. You can follow the progress of each disk image capture using the Automated Deployment Service MMC snap-in on the Controller server. In the MMC snap-in, explore Devices and Running Jobs to view the status of the capture tasks.

When the image captures are complete, ADS shuts down and removes the source system from the device database. The last task before the script terminates is changing system file attributes, as shown in Figure 10-2.

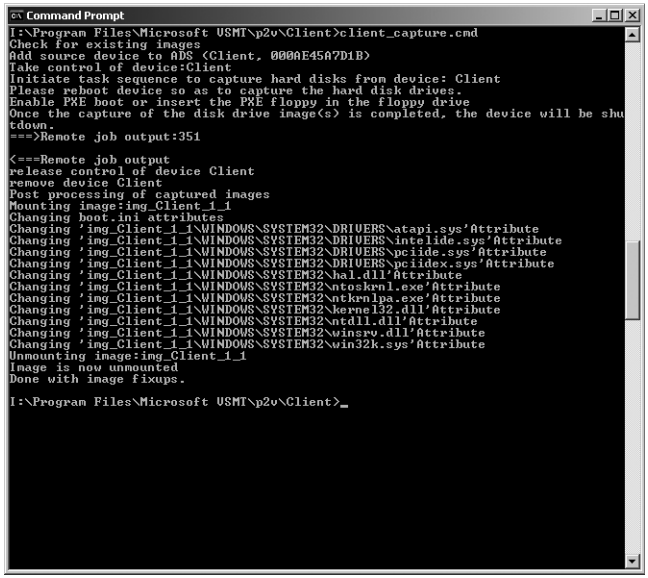

Figure 10-2 Sample output from the Source_capture.cmd script

Creating the Virtual Machine

The next step in the migration procedure is to execute the *Source*_CreateVM.cmd script and start the creation of the virtual machine in Virtual Server 2005 R2. Follow these steps to start the virtual machine creation:

1. Log on to the Controller server and open a command window.
2. In the command window, change the directory to the Virtual Server Migration Toolkit subdirectory where the generated migration files are stored.
3. In the command window, execute the *Source*_CreateVM.cmd script.

You can follow the progress of the virtual machine creation using the Virtual Server 2005 R2 Administration Website on the Controller server. You will see the creation of a new virtual machine configuration file, virtual machine creation, connection of the virtual machine to the default virtual network, creation and connection of the virtual hard disks to the virtual machine, and configuration of the virtual machine to attach an RIS virtual floppy drive.

When all these tasks are complete, check the ADS device database using the MMC snap-in. The virtual machine should have been added to the ADS device database and prepped for source system disk deployment. The script terminates after opening a browser window to the Virtual Server 2005 R2 Administration Website.

Deploying the Source System Disk Images to the Virtual Machine

After the virtual machine is created, the source system disk images must be restored to the attached virtual hard disks. The Source_DeployVM.cmd controls this part of the migration procedure. Follow these steps to restore the source system disk images and deploy the virtual machine:

1. Log on to the Controller server and open a command window.
2. In the command window, change the directory to the Virtual Server Migration Toolkit subdirectory where the generated migration files are stored.
3. In the command window, execute the Source_DeployVM.cmd script.

You can follow the progress of the virtual machine deployment using the Virtual Server 2005 R2 Administration Website on the Controller server. You will see the virtual machine boot into the Deployment Agent and the disk images restore to the virtual hard disks. The hardware-dependent system files are then swapped for virtual machine–compatible versions, and required operating system configuration settings are applied.

If you check the ADS device database using the MMC snap-in, you will see that the virtual machine is still in the device database. The script terminates after removing the RIS virtual floppy disk from the virtual machine. The virtual machine remains booted in the Deployment Agent.

Note You can specify the state of the virtual machine after deployment is complete by using the VMScript /postDeployAction parameter when generating the migration scripts. In this manner, you can choose to leave the virtual machine device in the Deployment Agent, restart the virtual machine, or shut down the virtual machine. If you decide to bring the virtual machine online, you will have to ensure that the physical server remains offline. Since both the physical server and virtual machine utilize the same SID, active directory computer account, and so on, conflicts arise if both machines are online simultaneously.

Completing the Migration Process

To complete the source system to virtual machine migration process, there are a few final tasks to perform:

1. Open the Virtual Server 2005 R2 Administration Website, and verify that the Event Viewer does not report any errors.
2. Open the Automated Deployment Services MMC snap-in, and send a reboot command to the virtual machine.
3. In the Automated Deployment Services MMC snap-in, release control and delete the virtual machine from the device database.
4. Log on to the virtual machine, and install the Virtual Machine Additions.
5. Complete any remaining virtual machine configuration modifications.
6. Test the virtual machine connectivity and performance to ensure that it is running as expected.

Important Once the virtual machine testing is complete, you can back up and delete the source system disk images from the Automated Deployment Services image store.

Performing a Virtual Machine to Virtual Machine Migration

You can use VSMT to migrate a VMware virtual machine to Virtual Server 2005 R2, provided that the VMware virtual machine is running one of the operating systems supported for migration. The migration procedure is the same as in the physical to virtual machine scenario. However, there are a couple of matters to consider prior to performing a VMware to Virtual Server virtual machine migration.

If the VMware virtual machine uses SCSI disks, you must copy the VMware SCSI drivers into the Automated Deployment Services file cache. Once you obtain the VMware SCSI drivers from the VMware Web site, follow the instructions in the "Loading Drivers into Automated Deployment Services" section earlier in this chapter.

Important If you encounter problems with the VMware SCSI drivers not loading correctly, there are two ADS hotfixes that you might have to apply to your installation. Review Microsoft Knowledge Base articles 829053 and 830413 found at *http://support.microsoft.com/kb/829053* and *http://support.microsoft.com/kb/830413*, respectively, for details.

In addition, you have to change the startup state of the VMware Tools Service to Disabled in the migrated virtual machine. Follow these steps to ensure that the VMware Tools Service is disabled automatically after the migration to Virtual Server 2005 R2:

1. Log on to the Controller server.
2. Using Windows Explorer, navigate to %systemdrive%\Program Files\Microsoft VSMT\Patches.
3. Right-click P2Vdrivers.xml and choose Edit.
4. Verify that the VMware Tools Service startup state is set to Disable.

The default P2Vdrivers.xml file specifies the startup state of drivers and services following the migration procedure. When generating the migration scripts, the VMScript.exe utility reads P2Vdrivers.xml and adds an entry in the generated task sequence that changes the start mode of the service or driver in the deployed virtual machine.

Summary

Before migrating a physical workload to a virtual machine, evaluate the workload memory, processor, network, and storage requirements to determine whether it is a good candidate for virtualization. To properly size the Virtual Server 2005 R2 physical host, consider the resource requirements of the host operating system in combination with the resource requirements of all the virtual machines that the system must support. A good rule of thumb is to add a 25-percent supplemental resource capacity to account for workload growth and additional virtual machines. Hardware and operational limitations must also be taken into account to ensure successful workload virtualization.

To understand the basic physical-to-virtual machine migration process, learn and use the free, downloadable VSMT in conjunction with ADS. Prior to starting the migration procedure, verify that the physical system configuration meets the requirements imposed by the tools. It is critical to review and understand the tools and scripts that are provided and created using the VSMT.

Once a migration procedure is complete, make sure to test the virtual machine under load to validate that performance and functionality meet production requirements. Finally, use VSMT to test the migration of virtual machines from VMware to Virtual Server 2005 R2.

Additional Resources

The following resources contain additional information related to the topics in this chapter:

- Knowledge Base article 829053, "Vendor-supplied drivers that you add to the ADS Deployment Agent Builder service repository are not installed," at *http://support.microsoft.com/kb/829053*
- Knowledge Base article 872952, "You cannot run the Chkdsk.exe program on NTFS file system volumes on a Windows NT 4.0 Service Pack 4-based computer," at *http://support.microsoft.com/kb/872952*
- Knowledge Base article 897614, "Windows Server System software not supported within a Microsoft Virtual Server environment," at *http://support.microsoft.com/kb/897614*
- Knowledge Base article 888794, "Considerations when hosting Active Directory domain controller in virtual hosting environments," at *http://support.microsoft.com/kb/888794*
- Knowledge Base article 830413, "The ADS Deployment Agent Builder Service does not correctly parse the latest .inf file formats," at *http://support.microsoft.com/kb/830413*
- Knowledge Base article 841550, "You receive an error message when you start a Windows Server 2003-based computer by using the ADS Deployment Agent," at *http://support.microsoft.com/kb/841550*
- Whitepaper, "Solution Accelerator for Consolidating and Migrating LOB Applications," at *http://www.microsoft.com/technet/solutionaccelerators/ucs/lob/lobsa/lobsaimg.mspx*
- Whitepaper, "Automated Deployment Services Technical Overview," at *http://www.microsoft.com/windowsserver2003/techinfo/overview/ads.mspx*
- Whitepaper, "Server Consolidation and Migration with VSMT," at *http://www.microsoft.com/windowsserversystem/virtualserver/overview/vsmtwhitepaper.mspx*
- ADS and VSMT Download, "Automated Deployment Services (ADS) 1.1," at *http://www.microsoft.com/downloads/details.aspx?FamilyID=d99a89c9-4321-4bf6-91f9-9ca0ded26734&DisplayLang=en*