

Microsoft

Server 2008

Applications Infrastructure

(70-643) Microsoft Certified
IT Professional (MCITP)



**Smarter
Training**

This LearnSmart Exam Manual covers the most important concepts you need to know in order to pass the Server 2008 Applications Infrastructure exam (70-643). By studying this guide, you will become familiar with an array of exam-related content, including:

- Deploying Servers
- Configuring Terminal Services
- Configuring a Web Services Infrastructure
- Configuring Network Application Services
- Navigating features related to Server 2008 R2
- And more!

Give yourself the competitive edge necessary to further your career as an IT professional and purchase this exam manual today!

Configuring Windows Server 2008 Applications Infrastructure (70-643) LearnSmart Exam Manual

Copyright © 2011 by PrepLogic, LLC.
Product ID: 012311
Production Date: September 6, 2011

All rights reserved. No part of this document shall be stored in a retrieval system or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein.

Warning and Disclaimer

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The publisher and authors assume no responsibility for errors or omissions. The information provided is on an “as is” basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this document.

LearnSmart Cloud Classroom, LearnSmart Video Training, Printables, Lecture Series, Quiz Me Series, Awdeeo, PrepLogic and other PrepLogic logos are trademarks or registered trademarks of PrepLogic, LLC. All other trademarks not owned by PrepLogic that appear in the software or on the Web Site (s) are the property of their respective owners.

Volume, Corporate, and Educational Sales

Favorable discounts are offered on all products when ordered in quantity. For more information, please contact us directly:

1-800-418-6789
solutions@learnsmartsystems.com

International Contact Information

International: +1 (813) 769-0920

United Kingdom: (0) 20 8816 8036

Abstract

This Exam Manual is intended to help information technology (IT) professionals prepare for the Windows Server 2008 Applications Infrastructure, Configuring (70-643) exam. The manual also includes newly-added material that describes Server 2008 R2 features and enhancements. To facilitate your training, there are charts, graphs and images to help you visualize some of the more complex topics presented and to help you better commit this information to memory. After passing this exam, candidates will obtain the Microsoft Certified Technology Specialist (MCTS) certification for 70-643. The candidate will also be one exam closer to becoming a Microsoft Certified IT Professional (MCITP) Enterprise Administrator.

What to Know

The Windows Server 2008 Applications Infrastructure, Configuring (70-643) exam will measure the candidate's ability to deploy servers, configure terminal services, configure web services, and configure network application services. The exam covers a lot of material included in the previously mentioned objectives. In addition, the exam tests candidates' knowledge of features related to Server 2008 R2. For this reason, candidates should have at least one year of experience implementing and administering a network operating system in a medium to large environment.

Below are the skills measured in this particular exam:

- Deploying Servers (28 percent)
- Configuring Remote Desktop Services (26 percent)
- Configuring a Web Services Infrastructure (25 percent)
- Configuring Network Application Services (21 percent)

Tips

This Exam Manual is not a comprehensive reference for IT professionals. It should be used as a quick reference study guide a few days prior to taking the exam. For candidates with less than one year of experience managing a network operating system, purchasing LearnSmart's Microsoft (70-643) Server 2008 Applications Infrastructure LearnSmart Video training is recommended. It is recommended for all IT professionals to purchase the practice exam associated with this Exam Manual.

Table of Contents

Abstract.....	3
What to Know	3
Tips	3
Domain 1: Deploying Servers.....	7
Deploy Images by Using Windows Deployment Services.....	7
<i>Installing WDS</i>	7
<i>Configuring WDS</i>	8
<i>Deploying Images</i>	13
Windows Deployment for Windows Server 2008 R2.....	17
<i>Windows Automated Installation Kit</i>	17
<i>Windows Deployment Services</i>	18
Configure Microsoft Windows Activation	20
<i>License Channels</i>	20
<i>Volume Activation Using MAK</i>	20
<i>Volume Activation Using KMS</i>	21
Configure Windows Server Hyper-V and Virtual Machines Virtualization and Hardware Requirements	23
<i>Installing and Configuring Hyper-V Server Role</i>	23
<i>Virtual Networking</i>	24
<i>Virtual Hard Disks</i>	24
<i>Backing Up and Restoring Virtual Machines</i>	25
<i>Optimizing Virtual Machines</i>	25
Configure High Availability.....	25
<i>Network Load Balancing</i>	25
<i>Failover Clustering</i>	28
Failover Clustering Enhancements in Windows Server 2008 R2	31
Configure Storage	35
<i>RAID Types</i>	35
<i>Network Attached Storage</i>	36
<i>iSCSI</i>	36
<i>Mount Points</i>	38

Domain 2: Configuring Terminal Services	38
Installing Terminal Services Server	38
Configuring Terminal Services Licensing	40
<i>Configure a License Mode for Terminal Server Role Service</i>	40
<i>Install a Terminal Services Licensing Server</i>	43
<i>Activate a Terminal Services Licensing Server</i>	43
Configuring Terminal Services Server Options	45
Configuring Terminal Services Client Connections	47
Configuring a Terminal Services Gateway	48
<i>Install the Terminal Services Gateway Service</i>	48
<i>Request a certificate for a Terminal Services Gateway server</i>	49
<i>Install a certificate on a Terminal Services Gateway server</i>	51
<i>Configure a TS Gateway CAP and a TS Gateway RAP</i>	52
<i>Configure a Remote Desktop Client to use a TS Gateway</i>	54
Configuring Terminal Services RemoteApp	56
<i>Deploy RemoteApp Programs through TS Web Access</i>	56
Configuring Terminal Services Load Balancing	60
<i>Install a TS Session Broker</i>	60
<i>Configure a TS Session Broker</i>	61
Configuring and Monitoring Terminal Services Resources	62
<i>Install Windows System Resource Manager</i>	62
<i>Configure Application Logging</i>	63
Terminal Services Gets a Facelift in Windows Server 2008 R2	64
Domain 3: Configuring a Web Services Infrastructure	65
Manage Internet Information Services (IIS)	65
<i>Installing IIS 7.0 on Windows Server 2008</i>	66
<i>Installing IIS 7.0 on Server Core</i>	66
<i>Configure IIS Delegation of Administrative Rights</i>	67
<i>Remote Management in IIS 7.0</i>	69
<i>IIS Configuration Backup</i>	71
<i>Configure IIS Logging</i>	72
<i>Health and Diagnostics</i>	74
<i>Tracing Feature</i>	74
<i>Using Command Line Tool APPCMD</i>	77

IIS 7.5	78
Manage Web Sites	78
<i>Create and Publish an IIS Web Site</i>	79
<i>Configure Virtual Directories</i>	80
Configure Web Site Authentication and Permissions	81
<i>Web Site Authentication</i>	81
<i>Web Site Authorization</i>	82
Configuring Web Applications	82
<i>Create a Web Application</i>	82
Configure SSL Security	83
<i>Request a Certificate for a Web Site</i>	83
<i>Install a Requested Certificate</i>	84
<i>Assign a Certificate to a Website</i>	85
Configure a File Transfer Protocol (FTP) Server	86
<i>Installing FTP</i>	86
<i>Starting the FTP Service</i>	86
<i>Creating a New FTP Site for Authenticated Users</i>	87
Configure Simple Mail Transfer Protocol (SMTP)	89
Domain 4: Configuring Network Application Services	91
Configure Windows Media Server	91
<i>Creating a Publishing Point</i>	92
<i>Caching and Proxy</i>	94
Configure Digital Rights Management (DRM)	94
Configuring Windows SharePoint Services	95
<i>Installing Windows SharePoint Services Stand-Alone</i>	96
<i>Installing Windows SharePoint Services Farm</i>	96
<i>Using STSadm</i>	97
<i>Antivirus</i>	97
<i>Configuring WSS Services Service Accounts</i>	99
<i>Configure WSS for E-mail Integration</i>	100
Practice Questions	103
Answers & Explanations	108

Domain 1: Deploying Servers

Deploy Images by Using Windows Deployment Services

Deployment-based solutions have been around for a number of years. Early solutions involved the use of answer files and captured images. Following that, the introduction of Remote Installation Services (RIS) made use of answer files and supported file-based deployments. File-based images were managed on RIS servers. This leads to the successor, Windows Deployment Services (WDS), the new and improved version of RIS. WDS provides a platform of components that will facilitate rapid deployments and the creation of your own custom deployment solutions.

Installing WDS

Administrators can install WDS by using the Initial Configuration Wizard, using the Server Manager Console, or using the command-line tool ServerManagerCmd.exe.

- Initial Configuration Wizard
 1. Click **Add roles** on the **Initial Configuration Tasks** screen.
 2. Click **Next**.
 3. Select **Windows Deployment Services**.
 4. Click **Next**.
 5. On the **Select Role Services** page, administrators have two role services to choose from for WDS.
 - ▶ **Deployment Server** – provides full functionality of configuring and deploying Windows operating systems remotely. Note that Deployment Server is dependent on the core components of Transport Server. Therefore, both options should remain selected. Both options are selected by default.
 - ▶ **Transport Server** – should be the *only* selected service if you do not want to integrate all of Windows Deployment Services functionalities. This option is useful for environments without AD DS, DNS, or a DHCP server. The core networking components are installed offering the ability to boot from the network using Pre-Boot Execution Environment (PXE) boot and Trivial File Transfer Protocol (TFTP).
 6. Click **Next**.
 7. On the **Confirmation Installation Selection** page, verify the roles, services, and modules are what you desire, then click **Install**.
- Server Manager
 1. In the **Roles Summary** pane, click **Add roles**.
 2. Click **Next**.
 3. Select **Windows Deployment Services**.
 4. Repeat above **Initial Configuration Wizard** steps.
- ServerManagerCmd.exe
 1. From the command prompt, run one of the following two commands:
 - ▶ For Deployment Server, run **ServerManagerCmd -install WDS**.
 - ▶ For Transport Server, run **ServerManagerCmd -install WDS-Transport**.

Configuring WDS

You must configure WDS after installing the server role. Once the WDS configuration has been completed, you will be able to add an install image and a boot image. Administrators can configure WDS by using the **WDSUTIL** command-line tool or **Windows Deployment Services MMC snap-in**.

- **WDSUTIL** – a powerful utility that can be used to automate WDS tasks by way of scripting. The following table contains a few commonly used WDSUTIL commands.

Command	Description
/add	Adds images, image groups, or pre-stages to WDS server.
/remove	Removes images, image groups, multicast transmissions, and namespaces from the WDS server.
/set	<p>Sets properties and attributes on an object.</p> <p>/set-Server - Configures the settings for a Windows Deployment Services server.</p> <ul style="list-style-type: none"> • [/DhcpOption60:{Yes No}] – Specifies whether DHCP option 60 should be configured for PXE. • [/PrestageUsingMAC:{Yes No}] – Specifies whether WDS should use the MAC address instead of the GUID to identify client computers.
/get	Retrieves properties and attributes about an object.

Table 1 - WDSUTIL Commands

Perform the following steps to configure a WDS server using the **Windows Deployment Services MMC snap-in**:

1. Navigate to **Start > Administrative Tools > Windows Deployment Services**.
 1. In the tree pane, expand **Servers**.
 2. Right click the WDS server and then select **Configure Server**.

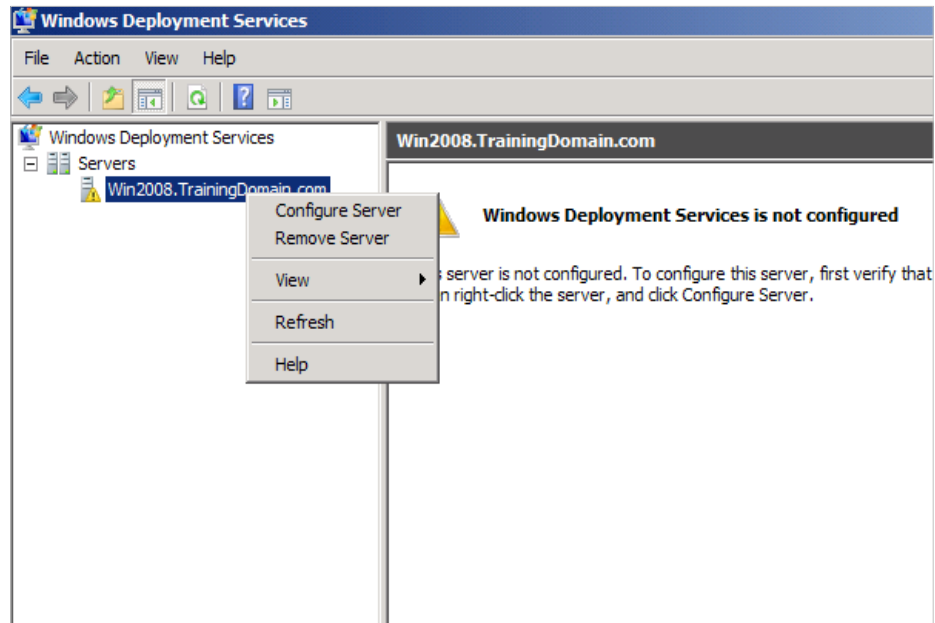


Figure 1 - WDS Configuring a Server

3. On the **Before You Begin** page, make sure the WDS configuration prerequisites are met.
 - ▶ The WDS server must be a member of an Active Directory Domain Services (AD DS) domain.
 - ▶ An active DHCP server must be on the network.
 - ▶ An active DNS server must be on the network.
 - ▶ The WDS server must contain an NTFS file system partition to store images.

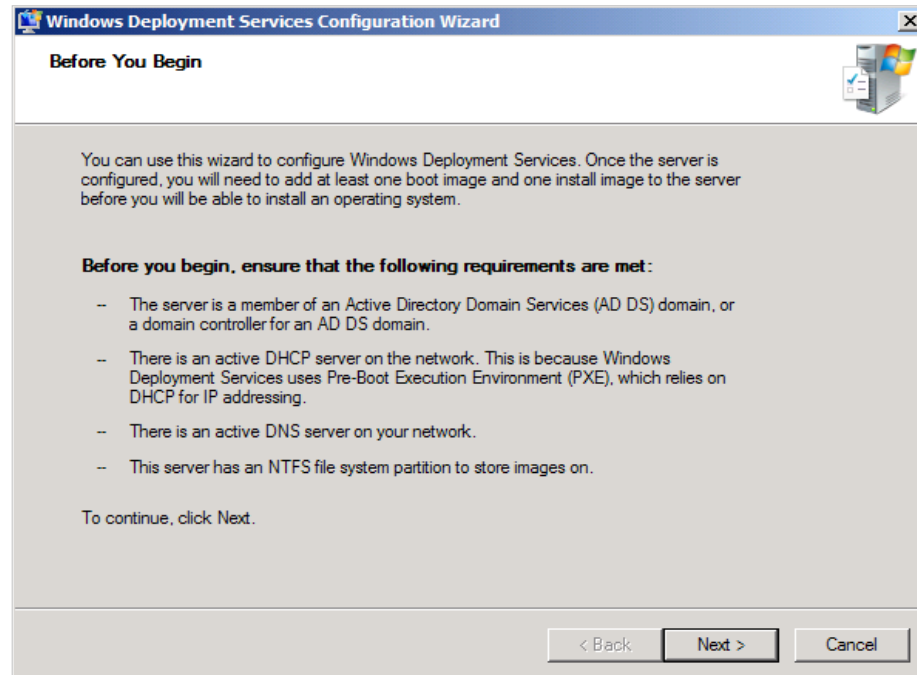


Figure 2 - WDS - Before You Begin

4. Click **Next**.
5. On the **Remote Installation Folder Location** page, specify a folder location for images, PXE boot files, and WDS management tools. The location must be on an NTFS partitioned drive and *should not* be the operating system partition.
6. On the **PXE Server Initial Settings** page, select the **Respond to all client computers (known and unknown)** option. Below is an explanation of the PXE Server Initial Settings options:
 - ▶ **Do not respond to any client computers** – disables the use PXE boot.
 - ▶ **Respond only to known client computers** – requires that each client have a computer account pre-staged in Active Directory.
 - ▶ **Respond to all client computers (known and unknown)** – allows any PXE boot compliant computer with proper domain credentials to retrieve images from the WDS server.
7. In this case, we will select **Respond to all client computers (known and unknown)**.
8. Click **Next**.
9. On the **Operation Complete** page, click **Finish**.
 - ▶ This page gives you the option to **install images to the server now**. If images are not available, you can simply uncheck the check box and install images later using the WDS snap-in.

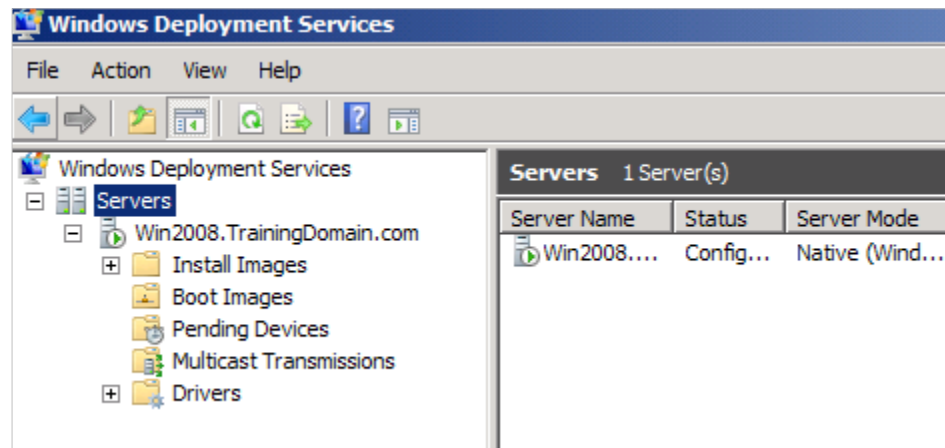


Figure 3 - WDS Installed

You will see several nodes listed under the WDS server once the Windows Deployment Services Configuration Wizard is done processing. The nodes include **Install Images**, **Boot Images**, **Pending Devices**, **Multicast Transmissions**, and **Drivers**.

1. **Install Images** – stores and provides administrators the ability to add install images (operating system images) to the WDS server for deployment.
2. **Boot Images** – stores and provides administrators the ability to add boot images to the WDS server for deployment.
3. **Pending Devices** – contains unknown computers which require administrator approval.
4. **Multicast Transmissions** – provides administrators the ability to create multicast transmissions on the WDS server. Using a single transmission, WDS will deploy the image to multiple computers.
5. **Drivers** – provides administrators the ability to add drivers to the WDS server.

At this point, you must verify and configure the properties of the server to complete the WDS configuration.

- Navigate to **Start > Administrative Tools > Windows Deployment Services**.
 1. In the tree pane, expand **Servers**.
 2. Right-click your server and then select **Properties**.

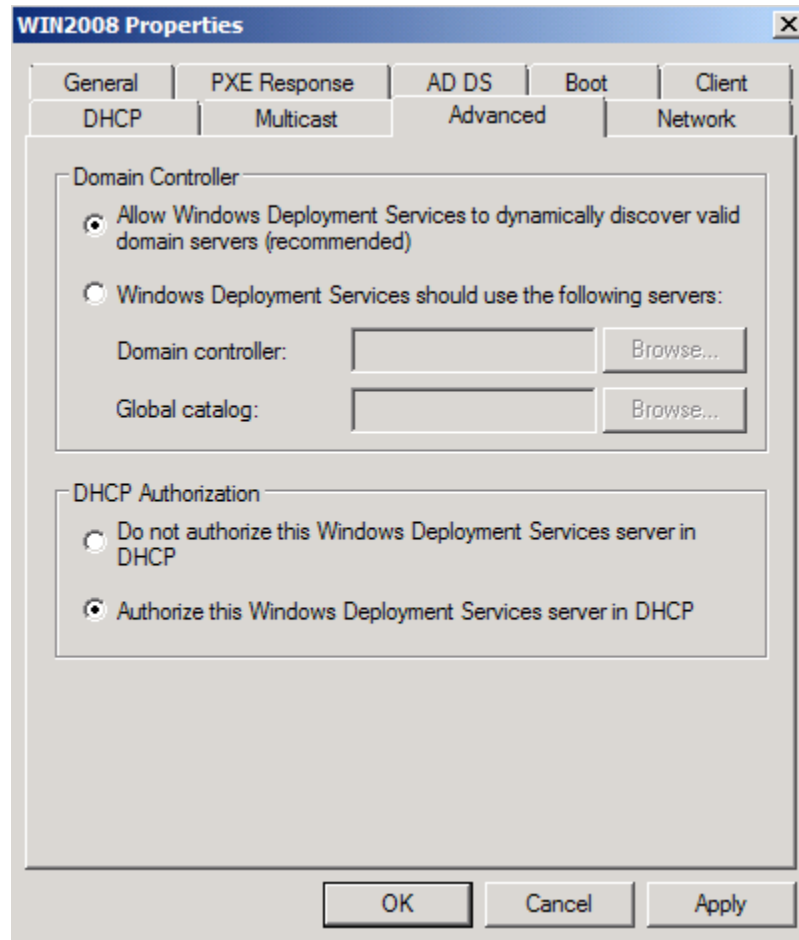


Figure 4 - WDS Properties Configuration - Advanced Tab

3. Click the **Advanced** tab and verify that **Allow Windows Deployment Services to dynamically discover valid domain servers** and **Authorize this Windows Deployment Services server in DHCP** are selected.

Note: The Deployment Server service requires AD DS, DNS, and DHCP in the environment in order to function. Remember, the Transport Server service does not require the above services if the Deployment Server service was not selected at the start of the installation process.

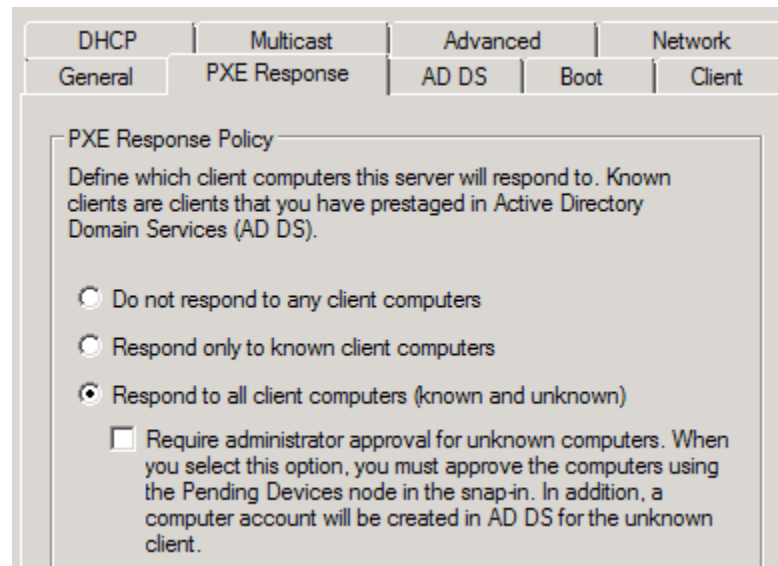


Figure 5 - WDS Properties Configuration - PXE Tab

4. Click the **PXE Response** tab and verify **Respond to client computer (known and unknown)** is selected.

Note: WDS will not respond to any clients if **Do not respond to any client computers** is selected. WDS will only respond to clients that are pre-staged in AD DS if **Respond only to known client computers** is selected. Many organizations deny the ability to join computers to the domain without first pre-staging them in AD DS. This is a best practice for the sake of security.

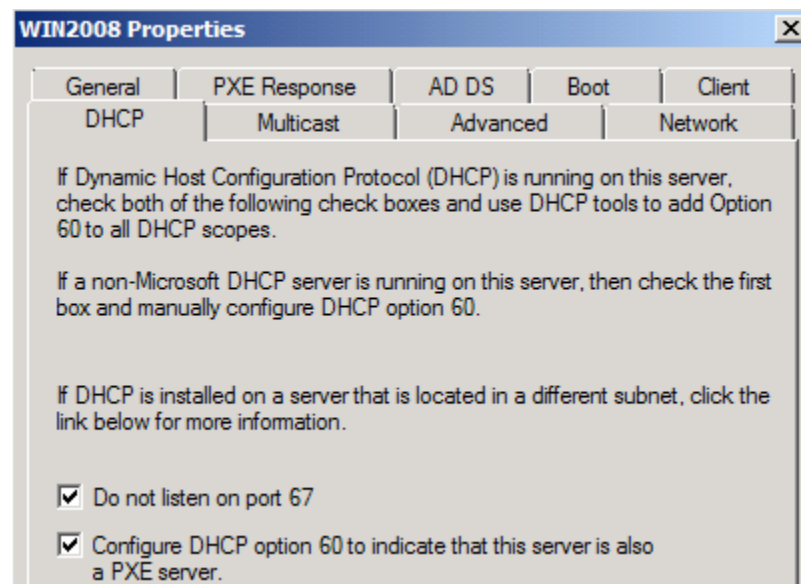


Figure 6 - WDS Properties Configuration - DHCP Tab

5. Click the **DHCP** tab and verify that options **Do not listen on port 67** and **Configure DHCP option 60 to indicate that this server is also a PXE server** are selected. Both options should be selected if DHCP is running on the WDS server, as the above figure indicates.

Deploying Images

Before deploying images, you must install images to the WDS server. WDS makes use of two fundamental image types, which uses the Windows Image (*.wim) file format. Your WDS server must contain at minimum one **install image** and one **boot image** before deploying operating systems to any PXE compliant computer.

- **Install image** – can be a customized image or a basic operating system image that administrators can deploy to client computers.
- **Boot image** – used to prepare a client computer for installation of an operating system image. The boot image contains the Windows Preinstallation Environment (Windows PE), which allows you to select from a list of install images. You can also build two other boot images—**capture image** and **discover image**.
 1. **Capture image** – used to capture the image of a reference client computer's operating system. Capture images contain the Windows Deployment Services Image Capture Wizard and Windows PE. At boot, the boot image stores the captured image as a .wim file.
 2. **Discover image** – an image stored on removable media that will discover WDS servers for non-PXE compliant clients. The image contains the Windows PE and WDS client.

Perform the following steps to store an **install image** on the WDS server:

- Navigate to **Start > Administrative Tools > Windows Deployment Services**.
 1. In the tree pane, expand **Servers**.
 2. Expand the appropriate WDS server.
 3. Right click the **Install Images** node, and then select **Add Install Image**.

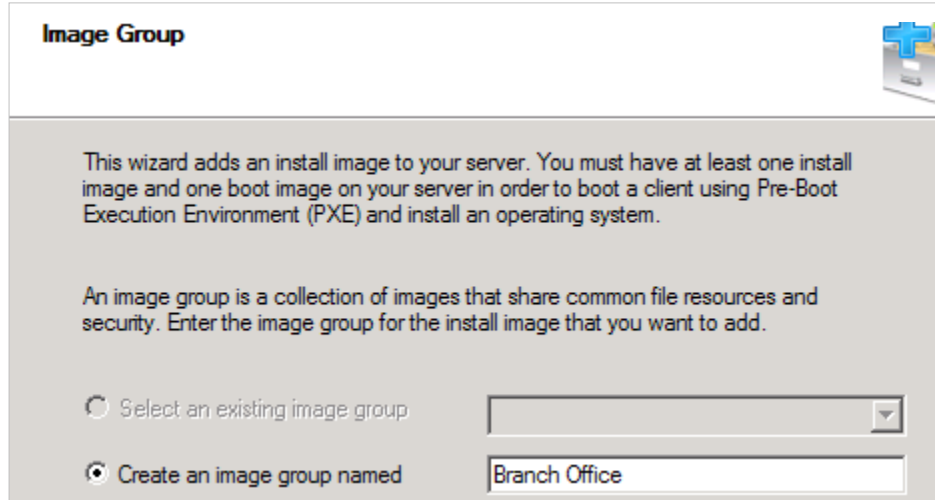


Figure 7 - Storing an Install Image on WDS

4. On the **Image Group** page, either select an existing image group or create an image group.
5. Click **Next**.

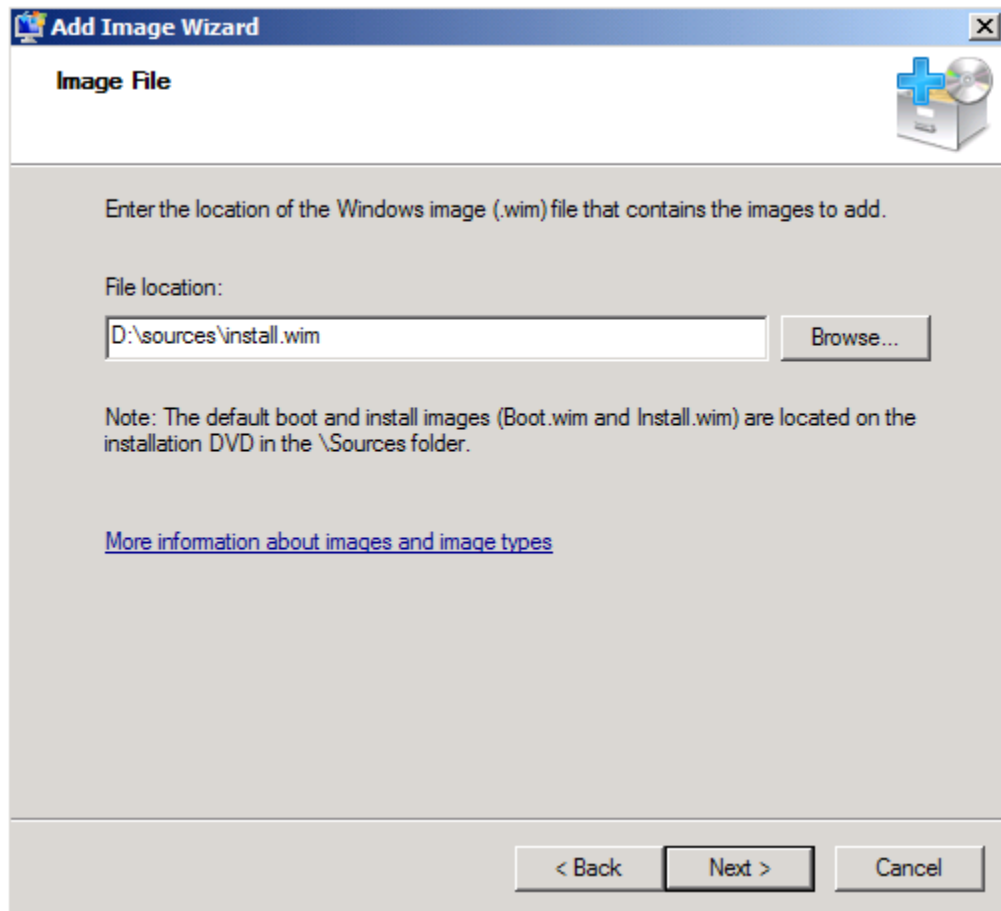


Figure 8 - Adding the Image

6. On the **Image File** page, type or browse to the file location of the install.wim file. The installation disk will contain multiple .wim files. You will see images for different versions of Windows. You will see 64-bit and 32-bit versions along with Standard and Enterprise.
7. Click **Next**.
8. On the **Available Images** page, select the image you want to add to the WDS server.
9. Click **Next**.
10. Review the **Summary** page and then click **Next**.
11. On the **Task Progress** page, once your selected images are uploaded to the WDS server, click **Finish**.

Perform the following steps to store a **boot image** on the WDS server:

- Navigate to **Start > Administrative Tools > Windows Deployment Services**.
 1. In the tree pane, expand **Servers**.
 2. Expand the appropriate WDS server.
 3. Right click the **Boot Images** node, and then select **Add Boot Image**.

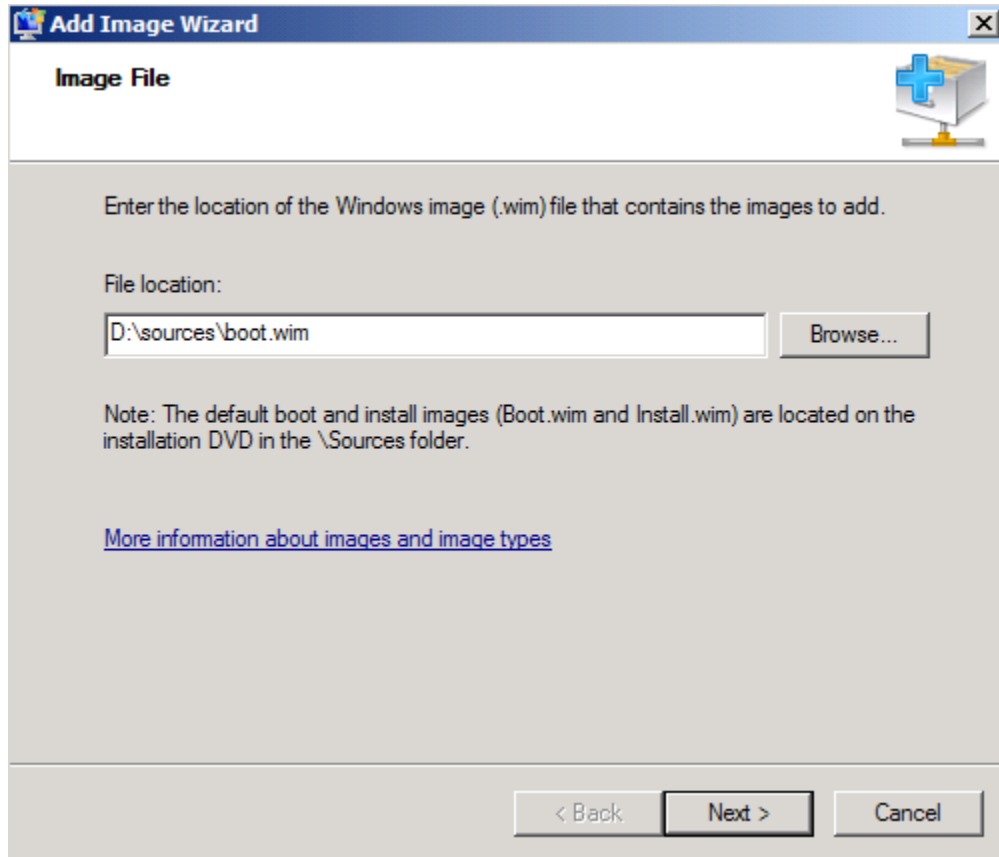


Figure 9 - Adding a Boot Image on WDS

4. On the **Image File** page, type or browse to the file location of the boot.wim file.
5. Click **Next**.

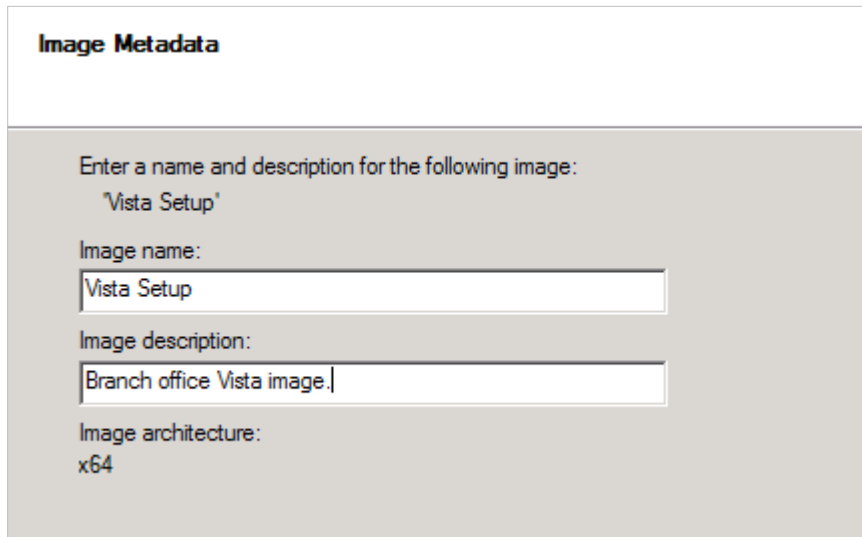


Image Metadata

Enter a name and description for the following image:
'Vista Setup'

Image name:

Image description:

Image architecture:
x64

Figure 10 - Inserting Image Metadata

6. On the **Image Metadata** page, enter an image name and image description.
7. Click **Next**.
8. Review the **Summary** page and then click **Next**.
9. On the **Task Progress** page, once your boot image is uploaded to the WDS server, click **Finish**.

Now the time has come to deploy an image to a client computer using PXE boot.

1. First, ensure the system is connected to the same network as the WDS server and DHCP server. If not, your network infrastructure team will have to configure DHCP Helper commands on one or more network devices.
2. Set the startup sequence to PXE boot your Network Interface Card (NIC) in the BIOS. The NIC should be first in the BIOS boot order.
3. Exit the BIOS and save changes. The system will then obtain a DHCP address. The address will be obtained either through port 60 or port 67.
4. If Network boot is not configured as an option in the BIOS, then press F12 to start the PXE boot process when prompted. The PXE client will contact and receive the boot image from the WDS server. Remember, the boot image contains Windows PE and the WDS client.
5. After Windows PE has loaded, you will need to select your **local** and **keyboard** configuration. Click **Next**.
6. An authentication window will open. You will need to authenticate using a domain and user account with proper credentials to complete the operation. Enter the correct format of **DOMAIN\UserName** and **password**.

Note: The Windows Automated Installation Kit (WAIK) offers the ability to automate these steps without touching thousands of computers.

1. On the **Install Windows** page, select the appropriate operating system.
2. On the next page, select the disk to install the operating system on and click **Next**.
3. The operating system installation will begin once the disk volume has been created and formatted.
4. At this point, the operating system will continue through the normal installation process until completion.

A successful deployment of a standard WDS Windows image has been accomplished.

Windows Deployment for Windows Server 2008 R2

Windows Server 2008 R2 adds new capabilities to the Windows deployment options available for the administrator. The majority of the changes fall into two categories:

- Windows Automated Installation Kit
- Windows Deployment Services

Windows Automated Installation Kit

The Windows Automated Installation Kit (WAIK) is used to create and deploy custom images of the Windows OS. Starting with Windows Server 2008 and Vista, all Windows OS installations are image-based. This simply means that the OS files are combined into a single large image file called a Windows Image (WIM). The WIM may also contain device drivers and scripts used for the automation of the installation. WAIK is a collection to tools and documented help that enables an administrator to customize his deployment environment.

The new version of the WAIK for Windows Server 2008 R2 and Windows 7 introduces a command line tool called DISM (deployment image servicing and management). DISM is a text-mode tool used to create and manage images. With it, you can install, uninstall, update and configure Windows drivers, features, packages and regional settings for an image. Additionally, you can use DISM commands to manipulate a running OS. The primary uses of DISM, for deployment, are to add or remove drivers, add or remove language packs, add and configure updates, and enable or disable Windows features.

In previous versions of WAIK, the functions of DISM were included in separate tools such as Package Manager (pkgmgr.exe), Windows PE command-line tool (PEimg.exe), and the International Settings Configuration Tool (intlcfg.exe). DISM is actually installed out-of-the-box with Windows Server 2008 R2 and Windows 7 as well.

The following table lists tools that were in the earlier versions of WAIK that no longer exist in the new version for Windows Server 2008 R2 and Windows Vista:

WAIK Tool	New Method
Intlcfg.exe	Was used to change language and locale settings. Now included in DISM.
PEimg.exe	Was used to create and modify Windows PE boot images. Now included in DISM.
Pkgmgr.exe	Was used to install and manage packages in an offline WIM image. Now included in DISM.
PostReflect.exe	Was used to reflect all boot-critical device drivers out of the driver store in an image. Now build-into SysPrep instead.
VSP1CLN.exe	Was used as the Vista SP1 File Removal Tool for removing files archived after installing Vista SP1. No longer available.

In addition to the DISM tool and the removal of several older WAIK tools, WAIK includes a new version of the User State Migration Tool (USMT). USMT 4.0 is used to perform user profile migration during large-scale deployments of either Windows Server 2008 R2 or Windows 7. The tool captures used settings, OS settings and application settings from the old system and migrates them over to the new platform.

The primary new feature of USMT 4.0 is the introduction of hard-link migration stores. With the hard-link migration store, you can perform an in-place migration without requiring a network location to store the profile information. All the user state is maintained on the computer, but the old OS is removed and replaced with Windows Server 2008 R2 or Windows 7.

Another important aspect of Windows Server 2008 R2 is the new support for BitLocker during installation. BitLocker was first introduced in Windows Vista and Server 2008 and it is used to encrypt storage volumes. In previous versions, you had to repartition your system after installation in order to enable BitLocker, if you had not manually partitioned the system for it during installation. Now, the default installation procedure creates an approximately 100 MB system partition that is available for BitLocker. The partition is not given a drive letter by default, but you can use the Windows System Image Manager (WinSIM) to modify this with the **Microsoft-Windows-Setup\DiskConfiguration\Disk\ModifyPartitions\ModifyPartition\Letter** setting.

The final element of WAIK and Windows deployment is the ability to use virtual hard disk (VHD) file for the running operating system. This is not unlike the old Stacker, SuperStore and DriveSpace technologies of the 1990s. One large file is created and the entire drive is stored within this file. The file is mounted as a virtual drive during system start and treated just like a physical drive. Files may be modified and the drive may be used as a normal physical drive would be. You can create bootable VHD files with the DiskPart tool or the Disk Management console in Windows.

NOTE: VHD files can also be mounted as drives within Windows systems. This allows you to mount a VHD file to a virtual machine for data storage and then shut down the virtual machine and mount the same VHD file to your local OS for data access.

Windows Deployment Services

Windows Deployment Services (WDS) is used to centrally store deployment images and allow for network-based deployments of the Windows OS. Windows Server 2008 R2 WDS supports the deployment of both Server 2008 R2 and Windows 7 images. In addition, it introduces several new capabilities that should be understood as you prepare for the 70-643 exam:

- **Dynamic driver provisioning**
Windows Server 2008 R2 allows for the dynamic addition of driver packages in the WDS server. When you add a driver package, you can deploy it to client computers based on the hardware in those computers as part of the installation. This can only be performed when installing images for Windows Vista with SP1, Windows Server 2008, Windows Server 2008 R2 or Windows 7. You can also add the driver packages to the Windows Server 2008 R2 or Windows 7 boot images. Dynamic driver provisioning eliminates the requirement of adding driver packages to images manually using the WAIK tools.

Driver packages can be placed into driver groups. The driver group can be filtered so that specific client computers can use them. The filters may be based on the hardware in the client, such as the manufacturer or BIOS vendor, or they may be based on the attributes on the install image, such as the version or edition of the image.

- Improved multicasting functionality**
 When deploying images using multicasting, you can now automatically disconnect slow clients. Additionally, you can divide transmissions into multiple streams depending on the client speeds. Grouping faster clients together and slower clients together provides for faster overall deployment times. IPv6 multicasting deployments are also now supported.
- Virtual hard disk deployment**
 In the preceding section, you learned that you can boot a physical machine to a VHD-based OS installation. WDS can also deploy these VHD images to the machines. However, while it cannot be used to deploy VHDs to virtual machines, it can be used to deploy VHDs to physical machines. Booting from VHD images allows you to provision a machine with multiple VHD images and then easily multi-boot between them for multi-purpose servers or clients.

VHD images are imported and configured using the WDSUTIL command. A complete reference to the WDSUTIL command is located at <http://go.microsoft.com/fwlink/?LinkId=89381>. However, the following table lists the important switches used in VHD management (parameters in square brackets are always optional as they have a default value):

WDSUTIL Parameter	Purpose
/ImageFile:<file path>	Defines the path and file name of the VHD file.
/Image:<image name>	Defines the name of the image on the WDS server.
[/Server:<Server name>]	Defines the name of the server. When no name is specified, the local server is used.
/ImageType:Install	Defines the fact that the image is an install image.
[/ImageGroup:<Image group name>]	Defines the name of the image group. When no name is specified, the source image file name is used.
[/Filename:<Filename>]	Specifies the image file name when required. When no name is specified, the source image file name is used instead.
/DestinationImage	Sets the parameters for the destination image such as the file path for the new image and whether the existing file should be overwritten, if it exists.
[/UnattendFile:<Unattend file path>]	Defines the path to the unattend file to use with the image. This file automates the installation.

- PXE provider for Transport Server**
 An additional role service, called the Transport Server, implements a PXE provider so you can network boot, multicast data, or both. The Transport Server is a stand-alone server as it does not require Active Directory or DNS.

To use the Transport server, you must perform three tasks. First, you must install the Transport Server role services. This is performed in Server Manager like any other role service. Next, you must prepare the files for network boot. To do this, you must create a share to store the boot files. Then, you must copy the boot files from an existing boot image to the share. The boot files are copied to the share using the DISM tool. Third and finally, you must configure the server. This involves adding a registry entry, creating an environment variable named REMOTEINSTALL, defining the TFTP server and then starting the Transport Server as described here [http://technet.microsoft.com/en-us/library/dd348475\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/dd348475(Ws.10).aspx).

Configure Microsoft Windows Activation

The growing software piracy pandemic affects many vendors on a daily basis. Volume license software is the main supply of illegal software. In an effort to reduce the software piracy footprint, Volume Activation (VA) 2.0 was introduced in Windows Vista and Windows Server 2008. VA 2.0 helps large organizations to better manage and protect their volume licenses. Multiple Activation Key (MAK) and Key Management Service (KMS) are components of VA 2.0 key management.

License Channels

Software licenses can be obtained through retail, original equipment manufacturer (OEM), or volume licensing.

- **Retail** - A retail license is a single license included with software purchases from a retail store. You must activate the software either online or by telephone.
- **OEM** - An OEM license ships with the hardware from the manufacturer. The license is preinstalled and no activation is required.
- **Volume Licensing** - Large corporations usually purchase volume licenses in bulk of five or more. Volume activation is performed through either Key Management Service Key (KMS) or Multiple Activation Key (MAK).

Volume Activation Using MAK

MAK offers two methods of activating clients.

- **MAK Independent** - MAK Independent activation uses a two-step process by which to activate clients.
 - Distribute the MAK key to a MAK client using one of the following methods:
 - Distribute using Volume Activation Management Tool (VAMT).
 - Distribute as a part of an image.
 - WMI script via GPO.
 - Distribute using the change product key wizard.
 - MAK client individually activates over the internet or by telephone.
- **MAK Proxy** - MAK Proxy activation is used to activate multiple MAK clients at the same time by way of a single connection to the internet. In other words, the MAK Proxy host, using the VAMT, connects to the internet on behalf of MAK clients.
 - **Volume Activation Management Tool** - VAMT is a graphical user interface tool that can activate both MAK Independent and MAK Proxy clients. The following bullet points describe the MAK Proxy client activation process:
 - VAMT discovers the MAK client from Active Directory or through discovery APIs.
 - VAMT obtains the installation ID and applies the MAK to the client.
 - VAMT connects to the internet and acquires the confirmation ID.
 - VAMT activates the MAK client using the confirmation ID.

Volume Activation Using KMS

Key Management Service provides local activation for clients in a corporate network. Using the KMS key, the KMS service is activated over the internet or by telephone. Once KMS has been completely configured and activated, clients can activate locally by connecting to the KMS service with no intervention. The below process describes the steps for installing and configuring KMS.

1. Designate one computer as a KMS host.
2. Input the product key into the KMS host server using the following command:

```
cscript %systemroot%\system32\SLMgr.vbs /ipk <KMS key>
```
3. The KMS host needs to connect to the internet and activate the KMS service using the following command:

```
cscript %systemroot%\system32\SLMgr.vbs /ato
```
4. Use the following command to activate the KMS by telephone:

```
%systemroot%\system32\SLUI.exe 4
```
5. Once the KMS service has started, it registers SRV locator records in DNS. This will allow clients to activate by locating KMS servers through DNS lookup. You can manually create SRV records by navigating to **Start > Administrative Tools > DNS**.

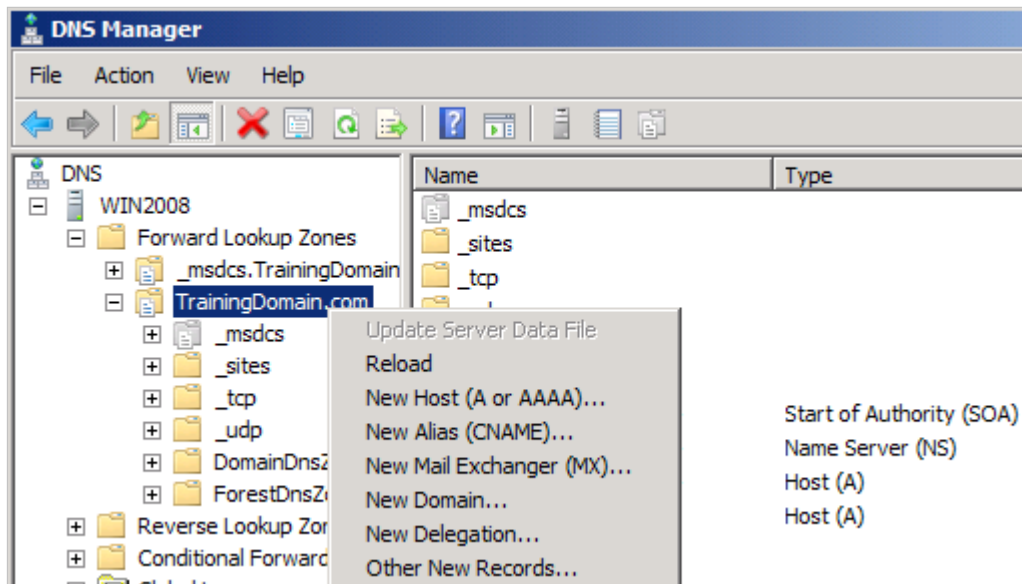


Figure 11 - Manually Creating SRV Records

1. Expand your DNS server.
2. Expand Forward Lookup Zones.
3. Right-click the appropriate domain and then select **Other New Records**.

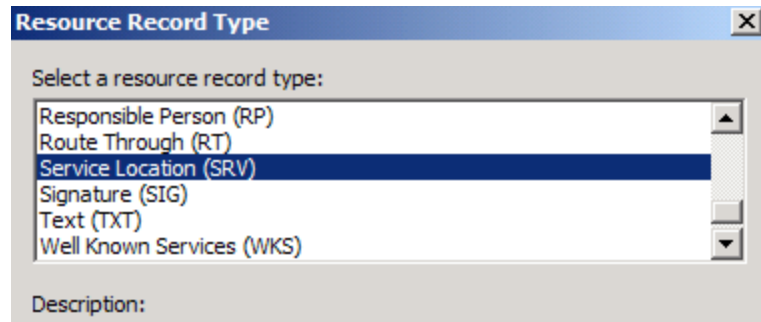


Figure 12 - Choosing the Record Type

4. In the **Resource Record Type** dialog box, select **Service Location (SRV)** and click **Create Record**.
5. In the **New Resource Record** dialog box, enter the following values and then click **OK**.
 - Service: **_VLMCS**
 - Protocol: **_TCP**
 - Port Number: **1688**
 - Host Offering This Service: **ServerName.FQDN**

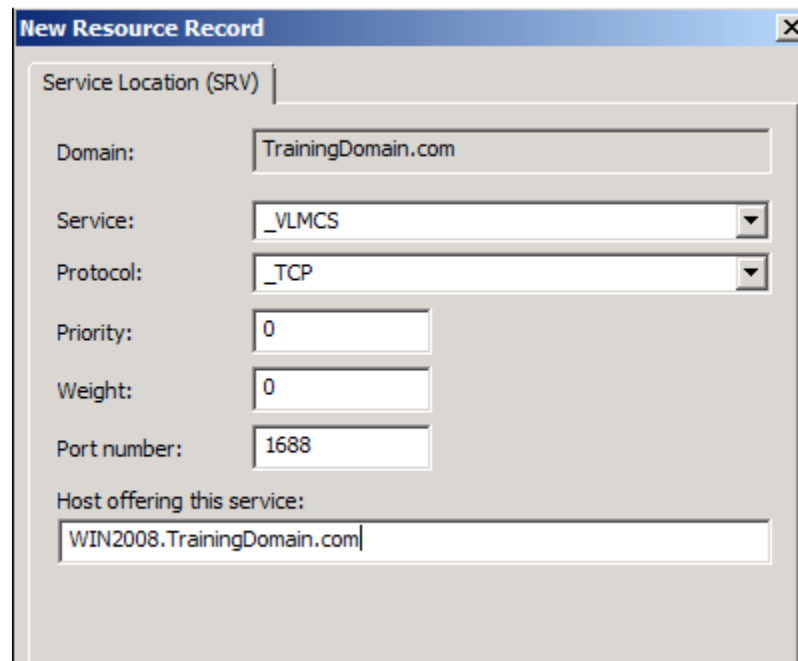


Figure 13 - Entering a New Resource Record

Out-of-the-box Windows Server 2008 and Windows Vista clients will automatically query DNS for a **_VLMCS** service record. Once located, the client will connect to the KMS host for activation.

Configure Windows Server Hyper-V and Virtual Machines Virtualization and Hardware Requirements

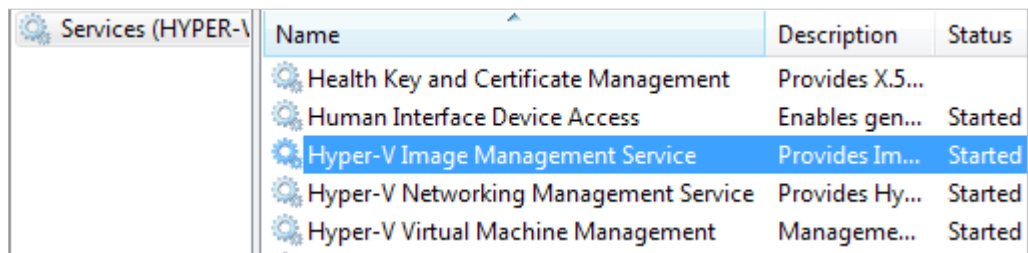
To install Hyper-V server role, you will need to adhere to particular hardware requirements. You will need the following:

- **Hardware-assisted virtualization** – you will need a processor that supports the virtualization option.
 - ▶ Intel VT
 - ▶ AMD-V
- **Hardware Data Execution Protection (DEP)** – DEP is required and must be enabled in the BIOS.
- **X64-based processor** - Hyper-V is available in the following x64-based Windows versions:
 - ▶ Windows Server 2008 Standard
 - ▶ Windows Server 2008 Enterprise
 - ▶ Windows Server 2008 Datacenter

Installing and Configuring Hyper-V Server Role

Once you have met the above specific hardware requirements, perform the following steps to install Hyper-V:

1. Navigate to **Start > Administrative Tools > Server Manager**.
 1. In the **Roles Summary** pane, click **Add Roles**.
 2. Click **Next**.
 3. Select **Hyper-V**.
 4. Click **Next** and follow the on-screen instruction to complete the **Add Roles Wizard**.
 5. At the end of the **Add Roles Wizard**, restart.



Name	Description	Status
Health Key and Certificate Management	Provides X.5...	
Human Interface Device Access	Enables gen...	Started
Hyper-V Image Management Service	Provides Im...	Started
Hyper-V Networking Management Service	Provides Hy...	Started
Hyper-V Virtual Machine Management	Manageme...	Started

Figure 14 - Adding the Hyper-V Server Role

6. Logon and verify Hyper-V services are running.
2. To enable Hyper-V on Server Core, execute the following command:


```
ocsetup Microsoft-Hyper-V
```
3. Restart when prompted.

Configuring your newly installed server role is done by adjusting Hyper-V settings. There are two groups of modifiable settings.

- **Server settings**
 - Virtual Hard Disks – indicates the default folder to store virtual hard disk files.
 - Virtual Machines – indicates the default folder to store virtual machine configuration files.
- **User Settings**
 - Keyboard – specifies how to use Windows key combinations when running Virtual Machine Connections.
 - Mouse Release Key – specifies the key combination you want to use to release the mouse.
 - User Credentials – identifies if you want to use default credentials automatically.
 - Delete Saved Credentials – specifies whether to cache or delete credentials once you disconnect from a running virtual machine.
 - Reset Check Boxes – resets all check boxes that were checked to hide pages and messages.

Virtual Networking

Hyper-V allows you to create three types of virtual networks:

- **Private Network** – only allow communications between virtual machines.
- **Internal Network** – allow communications between the Hyper-V server and virtual machines.
- **External Network** – by creating a connection to a physical network adapter, external virtual networks allow communications between a virtual machine and a physical network.

Perform the following steps to create a virtual network:

- Navigate to **Start > Administrative Tools > Hyper-V Manager**.
 1. From the **Actions** menu, click **Virtual Network Manager**.
 2. Under **Create virtual network**, select the type of network you want to create.
 3. Click **Add**.
 4. On the **New Virtual Network** page, type a name for the new network.
 5. Click **Apply**.

Virtual Hard Disks

Hyper-V uses .vhd files for virtual hard disks. Hyper-V gives you three types of hard disks to choose from when creating a virtual hard disk.

- **Dynamically Expanding** – disks grow as data is stored to the disk. It will only grow up to the size you indicated during configuration.
- **Fixed Size** – fixed sized disks will remain the same no matter how much data is stored on the virtual disk. You can use the Edit Virtual Hard Disk Wizard to adjust the size.
- **Differencing** – disks are associated with other virtual hard disks in a parent-child relationship. The .vhd file grows as adjustments are made to disk.

Backing Up and Restoring Virtual Machines

Disaster recovery is crucial to data availability and service reliability. Virtualizing core services is common practice in many organizations. Many of them realized the benefits of virtualization by migrating from physical to virtual (P2V). Some advantages of P2V are cost and up-time.

- **Cost** – organizations will reduce the long-term cost of hardware by migrating to a virtual environment.
- **Up-time** – with some form of backup solution in place, bringing virtualized servers down for maintenance will be invisible to customers.

There are many backup and restore solutions available for virtual machines. We will focus on Windows Server Backup utility and the Snapshot feature available in Hyper-V manager.

- **Windows Server Backup** – you must backup all associated volumes when backing up virtual machines using the Windows backup utility. Meaning that, if the virtual machine configuration file is stored on the f: volume and the .vhd file is stored on the e: volume, you must back up e: and f: for a successful restore.
- **Snapshot** – the Snapshot feature available in Hyper-V manager enables you to backup and restore virtual machines back to their original states.

Optimizing Virtual Machines

Like virtual machine additions for Virtual PC, Hyper-V Integration Services provides improved performance, improved control over input devices, improved network driver support, and much more. You need to consider memory and processor utilization prior to and after virtual machine installation.

- You must take note of previous performance on physical servers.
 - ▶ Identify the amount memory.
 - ▶ Identify CPU utilization.
- System Center Operations Manager (SCOM) can be used to gather and analyze performance information before and after your Hyper-V virtual machine installations.
 - ▶ You can better plan for your virtualization hardware resources.

Configure High Availability

Regardless of unplanned or planned outages, customers expect constant uptime. The reality is we live in a service-oriented society that demands that systems are online around the clock. This leads to the topic of discussion—high availability. The goals of high availability are to eliminate single points of failures and reduce downtime. High availability can be achieved through application redundancy and hardware redundancy.

Network Load Balancing

Network Load Balancing (NLB) is a way to combine the workload of multiple computers into one virtual cluster. NLB is most commonly implemented in server farms dispersing the incoming client requests to websites. The intent of NLB is to provide high scalability, high availability, and manageability.

- **Scalability** – defined as how well a solution to some problem can meet increasing performance demands. NLB does the following to support scalability:
 - ▶ Support up to 32 computer in a single cluster.
 - ▶ Balance request across multiple hosts.
 - ▶ Can remove hosts as workload decreases.

- **High Availability** – NLB provides high availability with very low downtime. To provide high availability, NLB can automatically:
 - ▶ Detect and recover from failed hosts.
 - ▶ Balance the workload when hosts are added or removed.
 - ▶ Recover the workload within ten seconds.

- **Manageability** – NLB provides the following:
 - ▶ Centralized management of multiple NLB clusters.
 - ▶ Different port rules for each service or application.
 - ▶ Logs to the Event Logs.
 - ▶ Remote administration.

Configuring NLB in Windows Server 2008 is fairly simple and straight to the point.

- Verify the Network Load Balancing feature has been enabled.
- Perform the following to create a new cluster:
 1. Navigate to **Start > Administrative Tools > Network Load Balancing Manager**.
 2. Right-click **Network Load Balancing Clusters** and click **New Cluster**.

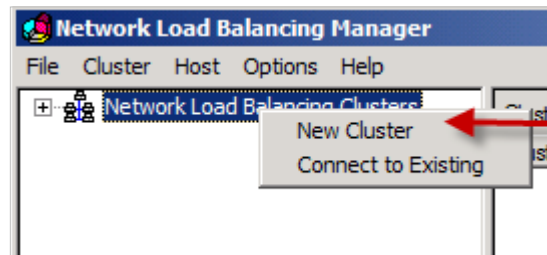


Figure 15 - Creating a New Cluster for NLB

3. In the **Host** text box, type the name of the host and click **Connect**.
4. Select the appropriate interface and click **Next**. This interface will host the virtual IP address. The virtual IP is the address clients will connect to and resolve in DNS. If one physical IP should become unavailable, NLB will load-balance between the other available physical IP addresses. The virtual IP can be associated to multiple interfaces.

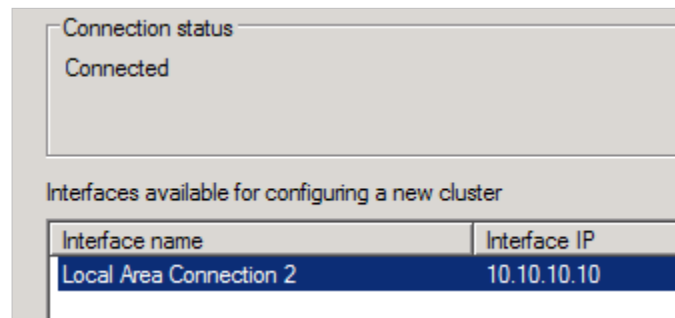


Figure 16 - Selecting an Interface

5. In the **Host Parameters**, select a value in **Priority**. This is the Unique Host Identifier. The host with the lowest priority is responsible for all traffic not detailed by a port rule.
6. Click **Next**.
7. In **Cluster IP Addresses**, click **Add** and then click **Next**. This will be the share cluster IP address.

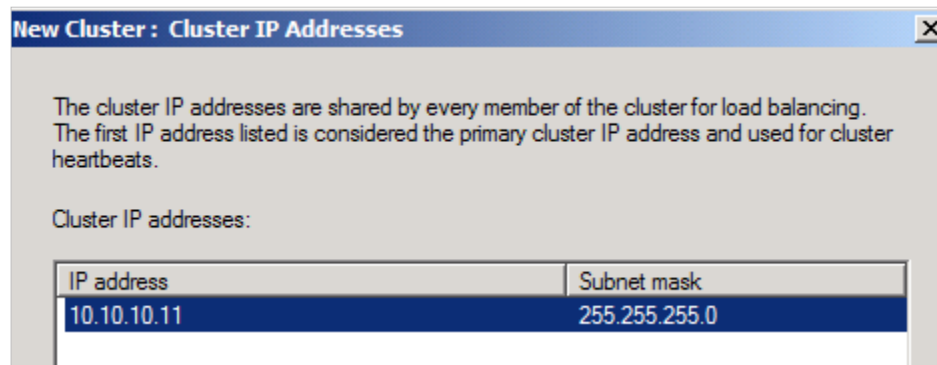


Figure 17 - Adding a Cluster IP Address

8. In the **Cluster Parameters**, configure the **Cluster IP configuration** and **Cluster operation mode**.
 - ▶ Under **Cluster IP configuration**, select the correct **IP address** and enter the **Full Internet name** that client will resolve.
 - ▶ Under **Cluster operation mode**, click **Unicast**. This will replace the physical MAC address with the unicast MAC.

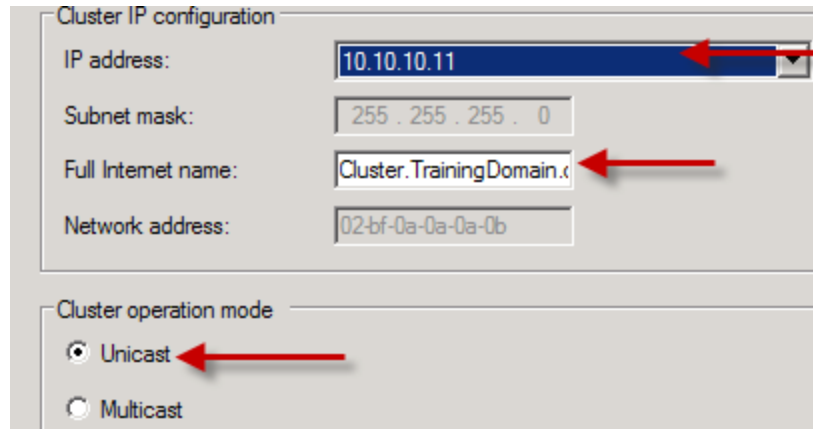


Figure 18 - Setting IP Address Parameters

Note: Unlike the **Unicast** selection, the **Multicast** selection allows hosts to retain its original MAC address. With that said, unicast hosts are not able to directly communicate with each other.

9. Click **Next**.
10. In **Port Rules**, click **Edit** if you need to modify port rules.

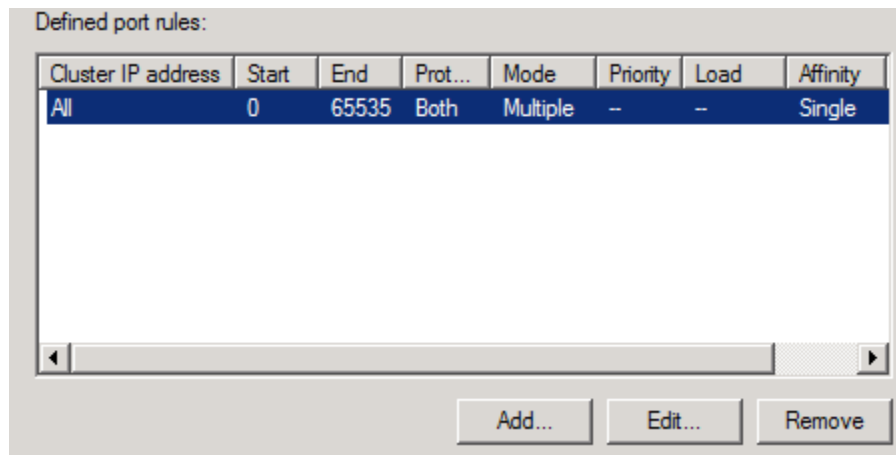


Figure 19 - Defining Port Rules

11. Click **Finish**.

Failover Clustering

A Failover cluster must adhere to specific requirements for software, hardware, and network infrastructure. Review the following software requirements for creating a failover cluster:

- All servers are required to either run the x64-based version or the Itanium architecture-based version of Windows Server 2008.
- Servers should have the same software updates and patches.
- Software cluster is included in the Windows Server 2008 Enterprise and Windows Server 2008 Datacenter, but not in Windows Server 2008 Standard or Windows Server 2008 Web Server.

Review the following hardware requirements for creating a failover cluster:

- **Servers** – use similar computers with the same hardware components.
- **Network Adapters** – adapters must be certified for Windows Server 2008. Network adapters should be dedicated to either network communication or iSCSI. A failover cluster cannot use both.
- **Device Controllers** – for SCSI or Fibre Channel, the mass storage device controllers must be one and the same.
- **Storage** – storage must be shared. The partition should be formatted with NTFS. The witness disk must be stored on an NTFS partition.

Review the following network infrastructure requirements for creating a failover cluster:

- For a failover cluster's network adapters, use identical communication settings.
 - ▶ Speed
 - ▶ Duplex Mode
 - ▶ Flow Control
 - ▶ Media Type

Perform the following steps to create a failover cluster:

- All nodes in the cluster must have the Failover Clustering feature installed prior to creating a failover cluster. Navigate to **Start > Administrative Tools > Server Manager**.
 1. Select the **Features** node and click **Add Features**.
 2. In the **Add Features Wizard**, select the **Failover Clustering** checkbox.

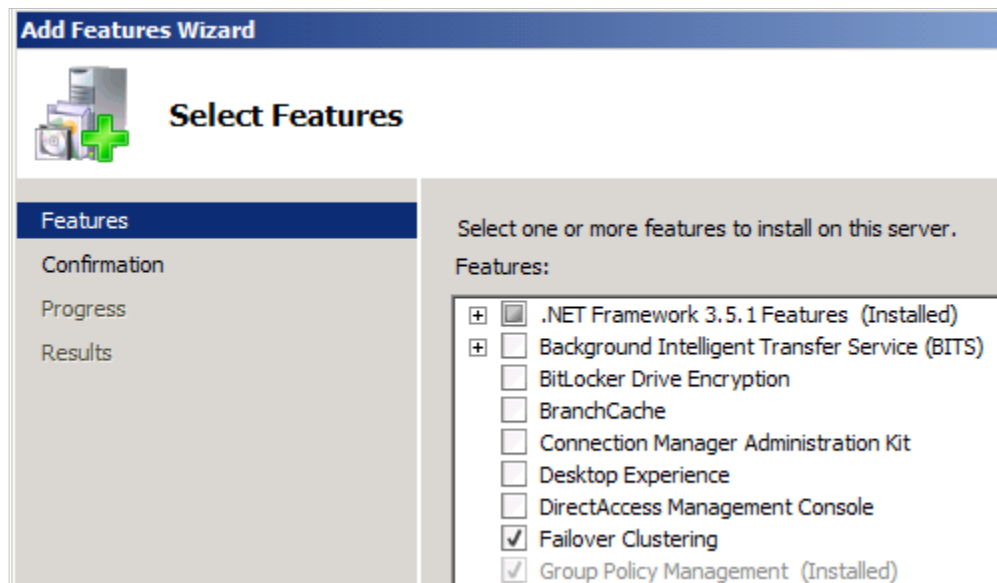


Figure 20 - Installing Failover Clustering

3. Click **Next**.
4. Confirm your installation and then click **Install**.

- Prior to creating a failover cluster, validate the cluster configuration.
 1. Navigate to **Start > Administrative Tools > Server Manager**.
 2. From the **Features** node, select **Failover Cluster Manager** and click **Validate a Configuration**.

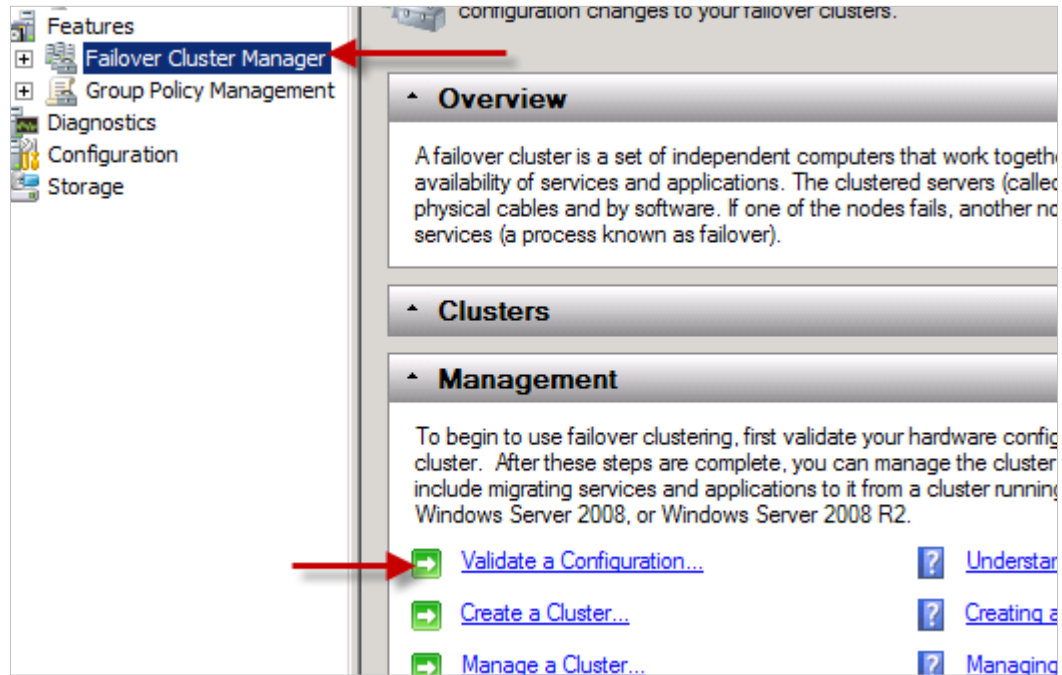


Figure 21 - Validating the Cluster Configuration

3. Click **Next**.
 4. On the **Select Servers or a Cluster** page, add the name of the cluster server to be verified and click **Next**.
 5. On the **Testing Options** page, select **Run all tests** and click **Next**.
 6. On the **Confirmation** page, click **Next**.
 7. View the report summary and click **Finish**.
- The next step is to execute the Create a Cluster Wizard.
 1. Navigate to **Start > Administrative Tools > Server Manager**.
 2. From the **Features** node, select **Failover Cluster Manager** and click **Create a Cluster**.
 3. Click **Next**.
 4. On the **Select Servers** page, add the name of the cluster server.
 5. On the **Select Servers** page, assign an IP address and name it, then click **Next**.

- The cluster has been created but now you need to configure the failover services by running the High Availability Wizard.
 1. Navigate to **Start > Administrative Tools > Server Manager**.
 2. From the **Features** node, select **Failover Cluster Manager** and click **Configure a Service or Application** in the action pane.
 3. On the **Before You Begin** page, click **Next**.
 4. On the **Select Service or Application** page, choose the application or service for which you want to provide high availability and click **Next**.

Note: Not all applications are cluster and failover aware. This section offers you the ability to configure generic applications for high availability.

1. Enter details of your chosen service and click **Next**.
2. View the summary report and click **Finish**.

Failover Clustering Enhancements in Windows Server 2008 R2

Like many other areas, Microsoft has made improvements to the failover clustering in Windows Server 2008 R2. One of the primary new improvements is the addition of several Windows PowerShell cmdlets for failover clusters. As with most server roles and features, Microsoft is gradually migrating administration over to PowerShell so that tasks may be scripted or performed through GUI interfaces that use the PowerShell backend.

To use the PowerShell cmdlets, you should import the FailoverClusters module using the Import-Module FailoverClusters command. After importing the module, you can use the Get-Command -Module FailoverClusters command to list the available cmdlets. The following table lists the cmdlets available as defined by Microsoft:

Cmdlet	Purpose
Add-ClusterDisk	Make a new disk available for use in a failover cluster. The disk (LUN) must be exposed to all nodes in the failover cluster, and should not be exposed to any other servers.
Add-ClusterFileServerRole	Create a clustered file server (resource group that includes one or more disks, on which you can create shared folders for users).
Add-ClusterGenericApplicationRole	Configure high availability for an application that was not originally designed to run in a failover cluster.
Add-ClusterGenericScriptRole	Configure an application controlled by a script that runs in Windows Script Host, within a failover cluster.
Add-ClusterGenericServiceRole	Configure high availability for a service that was not originally designed to run in a failover cluster.
Add-ClusterGroup	Add an empty resource group to the failover cluster configuration, in preparation for adding clustered resources to the group.
Add-ClusterNode	Add a node (server) to a failover cluster. Before adding the new node, you should run validation tests on the existing nodes together with the proposed new node.

Add-ClusterPrintServerRole	Create a clustered print server (a resource group that includes a printer and a disk for storing print job information and printer drivers).
Add-ClusterResource	Add a resource to a clustered service or application (resource group) in a failover cluster.
Add-ClusterResourceDependency	Add a resource to the list of resources that a particular resource depends on (using AND as the connector) within a failover cluster. Existing dependencies will remain in the list.
Add-ClusterResourceType	Add a resource type to a failover cluster, and specify information such as the dynamic-link library (DLL) to use with that resource type.
Add-ClusterServerRole	Add a group containing only a client access point and storage to the failover cluster configuration.
Add-ClusterSharedVolume	Make a volume available in Cluster Shared Volumes in a failover cluster.
Add-ClusterVirtualMachineRole	Create a clustered virtual machine, that is, a virtual machine that can be failed over if necessary to a different server in the failover cluster.
Block-ClusterAccess	Prevent the specified user or users from accessing a failover cluster.
Clear-ClusterDiskReservation	Clear the persistent reservation on a disk in a failover cluster.
Clear-ClusterNode	Clear the cluster configuration from a node that was evicted from a failover cluster.
Get-Cluster	Get information about one or more failover clusters in a given domain.
Get-ClusterAccess	Get information about permissions that control access to a failover cluster.
Get-ClusterAvailableDisk	Get information about the disks that can support failover clustering and are visible to all nodes, but are not yet part of the set of clustered disks.
Get-ClusterGroup	Get information about one or more clustered services or applications (resource groups) in a failover cluster.
Get-ClusterLog	Create a log file for all nodes (or a specific node) in a failover cluster.
Get-ClusterNetwork	Get information about one or more networks in a failover cluster.
Get-ClusterNetworkInterface	Get information about one or more network adapters in a failover cluster.
Get-ClusterNode	Get information about one or more nodes (servers) in a failover cluster.
Get-ClusterOwnerNode	For a resource in a failover cluster, get information about which nodes can own the resource. For a clustered service or application (a resource group), get information about the order of preference among owner nodes.

Get-ClusterParameter	Get detailed information about an object in a failover cluster, such as a cluster resource. This cmdlet is used to manage private properties for a cluster object.
Get-ClusterQuorum	Get information about the quorum configuration of a failover cluster.
Get-ClusterResource	Get information about one or more resources in a failover cluster.
Get-ClusterResourceDependency	Get information about the dependencies that have been configured between clustered resources in a failover cluster.
Get-ClusterResourceDependencyReport	Generate a report that lists the dependencies between resources in a failover cluster.
Get-ClusterResourceType	Get information about one or more resource types in a failover cluster.
Get-ClusterSharedVolume	Get information about Cluster Shared Volumes in a failover cluster.
Grant-ClusterAccess	Grant access to a failover cluster, either full access or read-only access.
Move-ClusterGroup	Move a clustered service or application (a resource group) from one node to another in a failover cluster.
Move-ClusterResource	Move a clustered resource from one clustered service or application to another within a failover cluster.
Move-ClusterSharedVolume	Move a Cluster Shared Volume to ownership by a different node in a failover cluster.
Move-ClusterVirtualMachineRole	Move the ownership of a clustered virtual machine to a different node.
New-Cluster	Create a new failover cluster. Before you can create a cluster, you must connect the hardware (servers, networks, and storage), and run the validation tests.
Remove-Cluster	Destroy an existing failover cluster. The affected servers will no longer function together as a cluster.
Remove-ClusterAccess	Remove a user from the access list on the cluster.
Remove-ClusterGroup	Remove a clustered service or application (also called a resource group) from a failover cluster.
Remove-ClusterNode	Remove a node from a failover cluster. After the node is removed, it no longer functions as part of the cluster unless you add it back to the cluster.
Remove-ClusterResource	Remove a clustered resource from the failover cluster.
Remove-ClusterResourceDependency	Remove a dependency between two resources in a clustered service or application within a failover cluster.
Remove-ClusterResourceType	Remove a resource type from a failover cluster.
Remove-ClusterSharedVolume	Remove a volume from the Cluster Shared Volumes in a failover cluster, and place it in Available Storage in the cluster.

Repair-ClusterSharedVolume	Run repair tools on a Cluster Shared Volume locally on a cluster node.
Resume-ClusterNode	Resume activity on a failover cluster node after you have suspended it (that is, paused it).
Resume-ClusterResource	Turn off maintenance for a disk resource or Cluster Shared Volume within a failover cluster.
Set-ClusterLog	Set the size and level of detail for the cluster log.
Set-ClusterOwnerNode	For a resource in a failover cluster, specify which nodes can own the resource. For a clustered service or application (a resource group), specify information about the order of preference among owner nodes.
Set-ClusterParameter	Control specific properties of an object in a failover cluster, such as a resource, a group, or a network.
Set-ClusterQuorum	Configure quorum options for a failover cluster.
Set-ClusterResourceDependency	Specify the resources that a particular resource depends on within a failover cluster. Existing dependencies will be overwritten by the dependencies that you specify.
Start-Cluster	Start the Cluster service on all nodes of the cluster on which it is not yet started.
Start-ClusterGroup	Bring one or more clustered services and applications (also known as resource groups) online on a failover cluster.
Start-ClusterNode	Start the Cluster service on a node in a failover cluster.
Start-ClusterResource	Bring a resource online in a failover cluster.
Stop-Cluster	Stop the Cluster service on all nodes in a failover cluster, which will stop all services and applications configured in the cluster.
Stop-ClusterGroup	Take one or more clustered services and applications (also known as resource groups) offline on a failover cluster.
Stop-ClusterNode	Stop the Cluster service on a node in a failover cluster.
Stop-ClusterResource	Take a resource offline in a failover cluster.
Suspend-ClusterNode	Suspend activity on a failover cluster node, that is, pause the node.
Suspend-ClusterResource	Turn on maintenance for a disk resource or Cluster Shared Volume so that you can run a disk maintenance tool without triggering failover.
Test-Cluster	Run validation tests for failover cluster hardware and settings. Tests can be run both before and after a cluster is set up.
Test-ClusterResourceFailure	Simulate a failure of a cluster resource.
Update-ClusterIPResource	Renew or release the DHCP lease for an IP address resource in a failover cluster.
Update-ClusterVirtualMachineConfiguration	Refresh the configuration of a clustered virtual machine within a failover cluster.

In addition to the PowerShell enhancements to failover clustering, Windows Server 2008 R2 makes the following changes:

- Support for more services in a cluster, including Distributed File System replication member servers and a Remote Desktop Connection Broker.
- Performance of live migrations of virtual machines that allows a virtual machine to move from one host to another in a way that typically allows the clients to maintain their connections to the virtual machine.
- The Cluster Validation Wizard performs additional tests called the cluster configuration tests. These tests verify that settings which affect how the cluster communicates across networks are configured appropriately.
- The new Migration Wizard can migrate settings from clusters running on Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2. The previous version could only migrate settings from Windows Server 2003 clusters. In addition to the settings it could migrate in previous versions, the Migration Wizard can also migrate settings from these resource groups:
 - Distributed File System Namespace (DFS-N)
 - Distributed Transaction Coordinator (DTC)
 - Internet Storage Name Service (iSNS) Server
 - Message Queuing (also called MSMQ)
 - Network File System (NFS)
 - Other Server (client access point and storage only)
 - Remote Desktop Connection Broker

Configure Storage

RAID Types

RAID may essentially be defined as: *two or more physical hard disks combined to make a single logical hard disk*. There are two forms of RAID:

- **Hardware RAID** – the more expensive of the two. It requires a disk controller connected to an attached storage or network storage.
- **Software RAID** – usually implemented in the operating system, which will result in an increase in CPU usage.

Windows Server 2008 utilizes RAID levels 0, 1, and 5. The operating system is typically stored on RAID 1 volumes. Improved write performance is an advantage RAID 5 has over RAID 1. Databases with high read/write activity are typically stored on RAID 5 volumes.

- **RAID 0 (Striped Volume)** – improves performance by distributing data across two or more disks. Striped volumes are dynamic volumes and offer no fault tolerance. In other words, if one drive fails, you lose all data. Perform the following steps to create a striped volume:
 1. In **Disk Management**, right-click the unallocated space on one of the dynamic disks.
 2. Click **New Striped Volume**.

- **RAID 1** (Mirrored Volume) – copies identical data to both drives. Operating systems are typically stored on RAID 1 volumes. Mirrored volumes are dynamic volumes and offer fault tolerance. If one drive fails, there is an exact copy of the operating system on the other mirrored volume. Perform the following steps to create a striped volume:
 1. In **Disk Management**, right-click the unallocated space on one of the dynamic disks.
 2. Click **New Mirrored Volume**.

- **RAID 5** (Striped with Distributed Parity Volume) – data and parity is dispersed across three or more disks. RAID 5 volumes are dynamic volumes and offer fault tolerance. If one drive fails, Windows Sever 2008 will repair the new drive using the parity bits. Perform the following steps to create a striped volume:
 1. In **Disk Management**, right-click the unallocated space on one of the dynamic disks.
 2. Click **New RAID 5 Volume**.

Network Attached Storage

A Network-Attached Storage (NAS) unit's sole purpose is to provide storage and shared file access to clients throughout the network. The NAS is not designed to provide day-to-day core services. NAS devices usually ships as a preconfigured hardware appliance. Accessing large files on the NAS appliance can pose a strain on network traffic. Therefore, for your more complex core services, a Storage Area Network (SAN) or block-based implementation is a better solution.

iSCSI

Internet Small Computer System Interface (iSCSI) is a technology that allows SCSI commands to be shared over the network by leveraging the Virtual Disk Specification (VDS) API. VDS is a set of distributed component object model (DCOM) interfaces used to configure disk storage. VDS can query and configure disks, volumes, host bus adapter (HBA) ports, and iSCSI initiators on remote systems. iSCSI is a simple and inexpensive network storage solution that enables hosts to connect to an iSCSI storage array using network interface cards (NICs). iSCSI is a more affordable alternative to Fibre Channel Area Networks. To configure iSCSI, you have to access the iSCSI Initiator Properties from administrative tools:

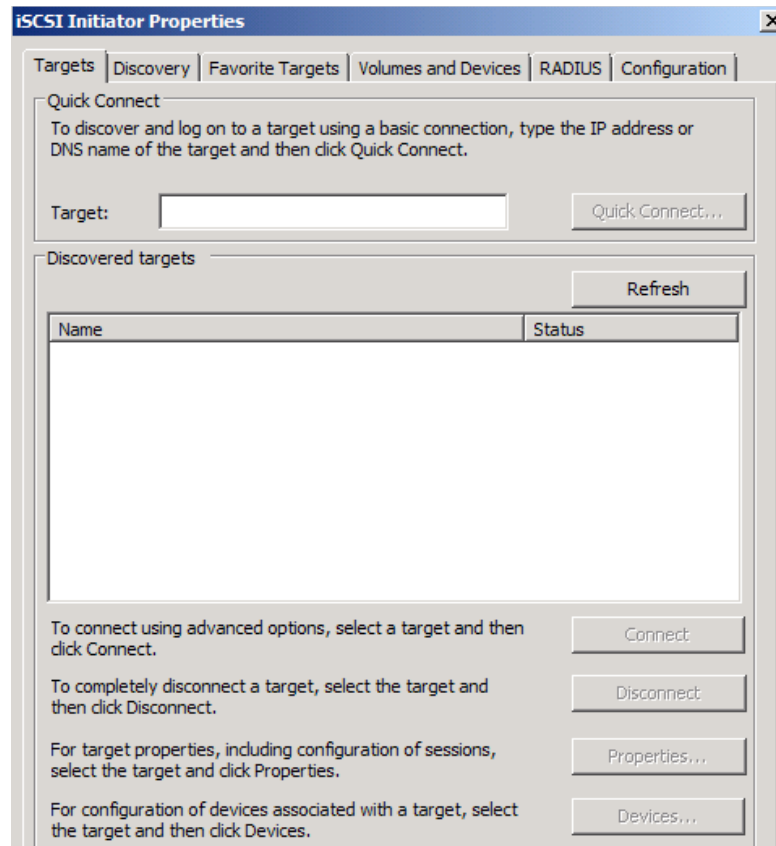


Figure 22 - iSCSI Initiator Properties

- **Targets** – here, you can initiate discovery by typing the name of the IP address of the target and make it a favorite location.
- **Discovery** – here, you can discover a target device and then make a connection to it on the **Targets** tab.
- **Volumes and Devices** – on this tab, you can add associated targets to the volumes list so that they are readily available for use by the service. The target must be on the favorite targets list.
- **RADIUS** – under these properties, you can add RADIUS servers to perform authentication for iSCSI connections.
- **Configuration** – here, you can modify the initiator name, set the initiator CHAP secret, or set up IPsec tunnel mode.

Mount Points

A mount point volume is a folder on a volume that has been assigned a drive path rather than a drive letter. Administrators typically separate drive letters by role for increased performance. Unfortunately, this poses a risk of running out of drive letters. To mitigate this risk, use mount points instead of drive letters to separate roles.

- Perform the following steps to create a mounted drive:
 1. In **Disk Manger**, right-click the volume you want to mount.
 2. Click **Change Drive Letter and Paths**.
 3. Click **Add** to mount a volume and browse for an empty NTFS folder.
 4. Locate the folder and click **OK**.

Note that when you create a volume mount point on a Windows Server 2008 failover cluster, it must be created on either a clustered disk or a nonclustered disk, not both. You have successfully created a volume mount point.

Domain 2: Configuring Terminal Services

The Terminal Services server in a Windows Server 2008 environment allows users access to specific applications or the entire Windows desktop environment. Users can access the Terminal Services server either by using the Remote Desktop (RDP) Client or over the Internet. Terminal Services is made up of the following configurable components called role services:

- **Terminal Server** – enables access to applications and to the entire Windows desktop environment.
- **Terminal Services Licensing (TS Licensing)** – manages the Terminal Services Client Access License (TS CAL) for users and devices.
- **Terminal Services Gateway (TS Gateway)** – enables users, with proper credentials, access to internal resources from computers over the internet.
- **Terminal Services Web Access (TS Web Access)** – allows access to RDP-enabled computers and RemoteApp programs through the TS Web Access website.
- **Terminal Services Session Broker (TS Session Broker)** – enables session load balancing between terminal servers in a farm.

Installing Terminal Services Server

Before configuring a TS Licensing role service, a TS Gateway role service, a TS Web Access, or a TS Session Broker roles service, you need to first install the Terminal Services server role. Perform the following steps to install a Terminal Services server role:

- Navigate to **Start > Administrative Tools > Server Manager**.
 1. In the **Roles Summary** pane, click **Add Roles**.
 2. Click **Next**.

- On the **Select Server Roles** page, select the **Terminal Services** check box.

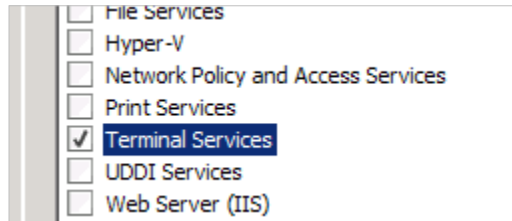


Figure 23 - Installing the Terminal Services Server Role

- Click **Next**.
- On the **Terminal Services** page, click **Next**.
- On the **Select Roles Services** page, select the **Terminal Server** check box.

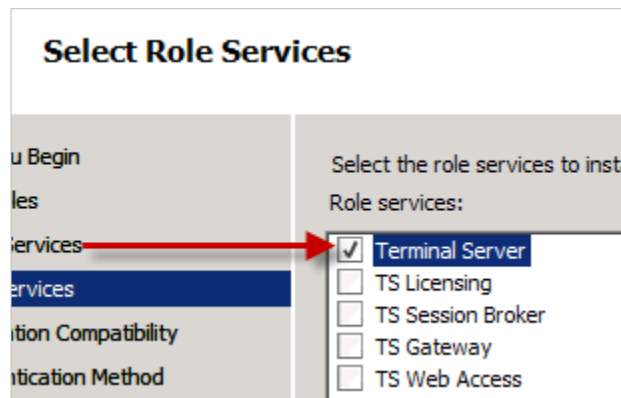


Figure 24 - Installing the Terminal Server Role Service

- Click **Next**.
- On the **Uninstall and Reinstall Applications for Compatibility** page, click **Next**.

Note: This is a message page that warns about the possibility of reinstalling applications that are not already installed.

- On the **Specify Authentication Method for Terminal Server** page, you have two options:
 - ▶ **Require Network Level Authentication** – computers that are running a supported version of at least Remote Desktop Client 6.0 should select this setting.
 - ▶ **Do not require Network Level Authentication** – all versions of Remote Desktop Client support this setting. This option is not as secure as Network Level Authentication.
- Select **Require Network Level authentication**, and then click **Next**.
- On the **Specify Licensing Mode** page, you have three options:
 - ▶ **Configure later** – select this option if you are not sure which license path you will take.
 - ▶ **Per Device** – allows an unlimited number of users, using a single device, to connect to a Terminal Server.
 - ▶ **Per User** – allows a limited number of users, bound by the number of licenses, to connect to a Terminal Server from an unlimited number of devices.

12. Select **Configure later**, and then click **Next**. We will configure a licensing mode later on in this chapter.
13. On the **Select User Groups Allowed Access to This Terminal Server** page, add the appropriate group and then click **Next**.
14. On the **Confirm Installation Selections** page, verify the summary and then click **Install**.
15. On the **Installation Results** page, click **Close**, and then **Yes** to restart.
16. Upon restart, Windows Server 2008 will resume configuring Terminal Services.
17. Once the configuration is complete, review the results summary and click **Close**.

Configuring Terminal Services Licensing

After installing the Terminal Server Role Service, perform the following steps to configure Terminal Services Licensing: configure the License Mode, install a Terminal Services Licensing Server, and activate the Terminal Services Licensing Server.

Configure a License Mode for Terminal Server Role Service

The TS Licensing role service installs and manages TS CAL for users and devices connecting to terminal servers. Note that RDP allows two simultaneous connections without the need of a TS CAL. Before configuring TS Licensing, decide on the type of TS CALs your organization will purchase and make available on the TS Licensing server. The type of TS Licenses available on the TS Licensing server must match the license mode configuration. Note that previous versions of Windows did not offer the ability to track TS per User CALs. You can use the TS Manager Licensing tool in Windows Server 2008 to track TS per User CALs. There are two types of TS CALs:

- **TS Per User CALs** – gives users unlimited access to terminal servers from any computer on the network.
- **TS Per Device CALs** – issued to devices the second time it connects to the terminal server. The first time a device connects to a terminal server, a temporary license is issued.

Next, decide on the type of discovery scope that you will implement on your TS Licensing server. Terminal servers that are not joined to a domain but are in the same workgroup can discover the configured license server—this is a **workgroup** discover scope. Terminal Servers that are members of the same domain can discover the configured license server—this is a **domain** discovery scope. Terminal Servers that are members of multiple domains in the same forest can discover the configured license server—this is a **forest** discovery scope.

- Perform the following procedures to configure a license mode for a Terminal Services server:
 1. In the **Terminal Services Configuration** dialog box, right-click **Terminal Services License Mode** and click **Properties**.

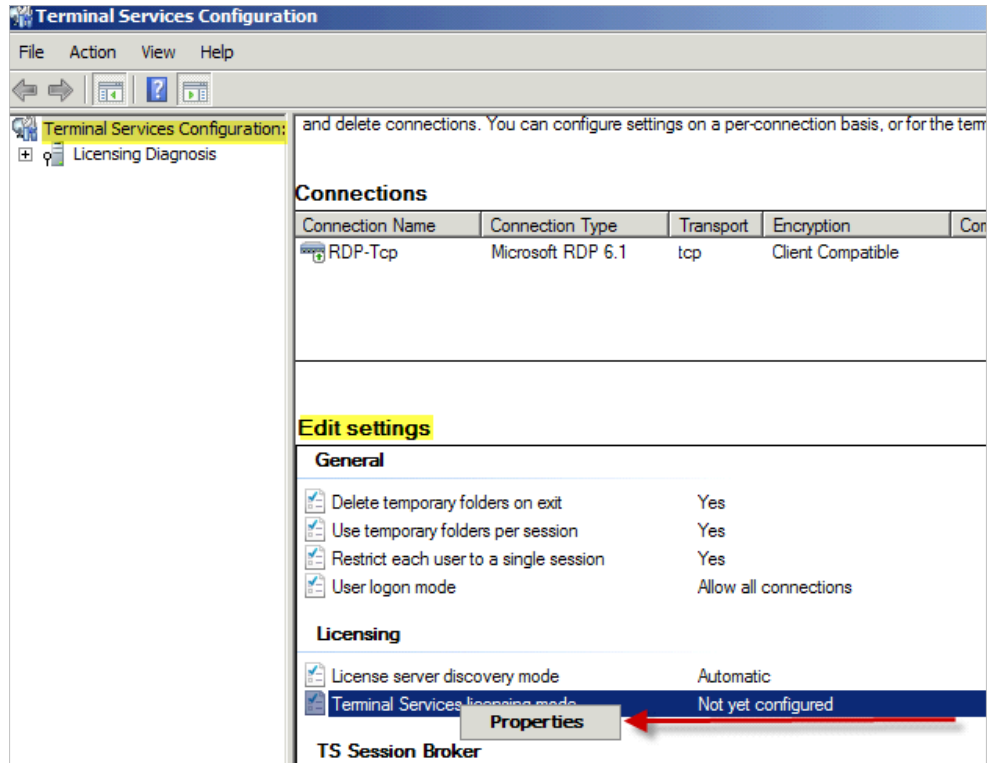


Figure 25 - Opening TS Licensing Properties

2. On the TS licensing mode windows, under the **Specify the Terminal services licensing mode** section, you have three options:
 - ▶ **Not yet configured** – select this option if you are not sure which license path you will take.
 - ▶ **Per Device** – allows an unlimited number of users, using a single device, to connect to a Terminal Server.
 - ▶ **Per User** – allows a limited number of users, bound by the number of licenses, to connect to a Terminal Server from an unlimited number of devices.

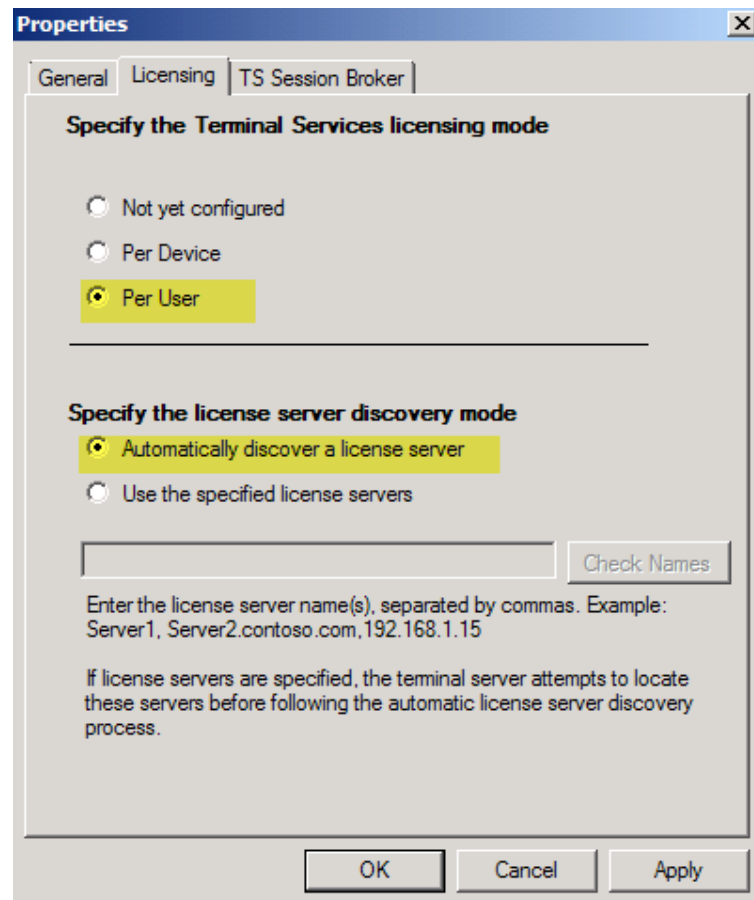


Figure 26 - Specifying a TS Licensing Mode

3. Select **Per User**.
4. On the TS licensing mode windows, under the **Specify the license server discovery mode** section, you have two options:
 - ▶ **Automatically discover a license server** – during license server discovery, a Terminal Server attempts to find and connect to a license server in the following order: license servers that are configured in the Terminal Services Configuration; a license server that is configured on the same computer as the terminal server; license servers published in Active Directory; and then license servers installed on domain controllers.
 - ▶ **Use the specified license servers** – before utilizing the “Automatically discover a license server” method, the Terminal Server will attempt to connect to license servers configured in this setting.
5. Select **Automatically discover a license server**, and then click **Apply**.

Install a Terminal Services Licensing Server

The Terminal Server Licensing role service can be installed on the same server as the Terminal Server role service. It is, however, recommended that the TS Licensing role service be installed on a separate server.

- To install a TS Licensing server, perform the following:
Navigate to **Start > Administrative Tools > Server Manager**.
 1. In the **Roles Services** pane, click **Add Role Services**.
 2. On the **Select Role Services** page, select **TS Licensing** and click **Next**.
 3. On the Configure Discovery Scope for TS Licensing page, as stated previously you have three options:
 - ▶ **Workgroup** – Terminal Servers that are not joined to a domain but are in the same workgroup can discover the configured license server.
 - ▶ **Domain** – Terminal Servers that are members of the same domain can discover the configured license server.
 - ▶ **Forest** – Terminal Servers that are members of multiple domains in the same forest can discover the configured license server.
 4. Select **Domain**, and then click **Next**.
 5. On the **Confirm Installation Selection** page, verify the settings and click **Install**.
 6. On the **Installation Results** page, verify the results and click **Close**.

Activate a Terminal Services Licensing Server

Before your TS Licensing server will begin issuing TS CALs, you must activate the server. You can activate your TS Licensing server through a web browser, a telephone, or an automatic connection over the internet. Use the automatic connection method if you have a connection the Internet from the license server. The server will update the required information over the Internet. Use the web browser method if you only have Internet access from another computer. Use telephone method if you have no Internet connectivity.

- To activate a Terminal Services Licensing server, perform the following method: Navigate to **Start > Administrative Tools > Terminal Services > TS Licensing Manager**.
 1. In the right pane, right-click the license server you want to activate, and then click **Activate Server**.

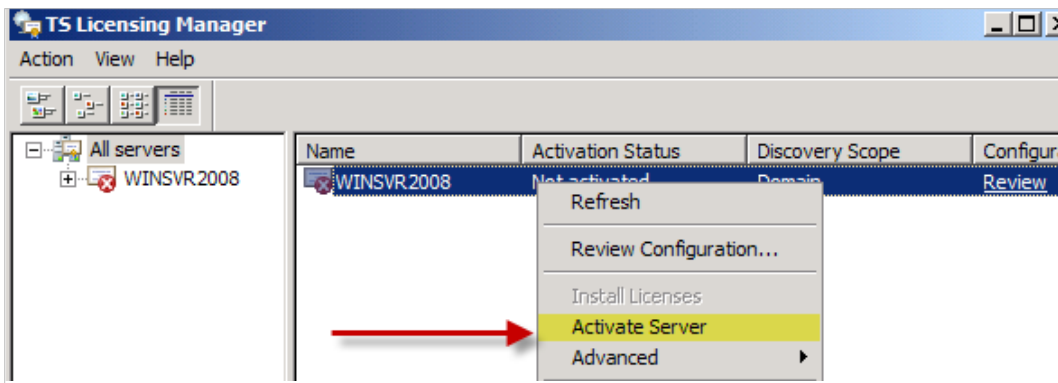


Figure 27 - Activating the TS Licensing Server

2. On the **Activate Server Wizard** page, read the page and then click **Next**.
3. On the **Connection Method** page, you have three activation connection options:
 - ▶ **Automatic connection** – use this method if you have a connection the Internet from the license server. The server will update the required information over the Internet.
 - ▶ **Web Browser** – use this method if you only have Internet access from another computer.
 - ▶ **Telephone** – use this method if you have no Internet connectivity.

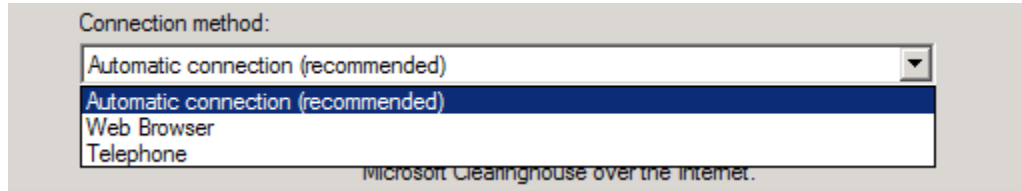


Figure 28 - Selecting the Connection Method

4. Select **Automatic connection** and then click **Next**.
5. The license server will attempt to locate a Microsoft activation server.

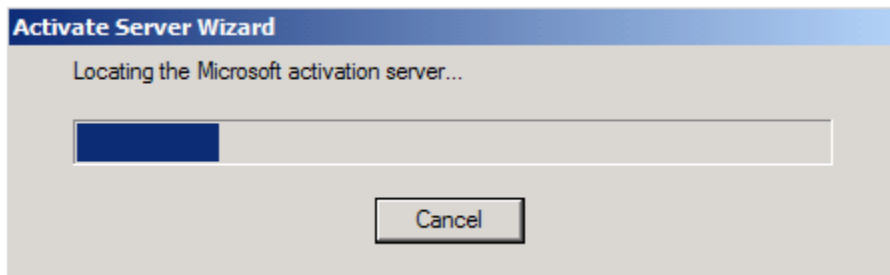


Figure 29 - Locating the Activation Server

6. Complete the **Activate Server Wizard** by entering your company information.

Configuring Terminal Services Server Options

Using Terminal Services Configuration, you have granular control over client connections to the terminal server. These settings include but are not limited to security layer and encryption, session time limits, and log on settings.

To configure Terminal Services server options, perform the following: Navigate to **Start > Administrative Tools > Terminal Services > Terminal Services Configuration**.

- In the **Terminal Services Configuration** dialog box, right-click the **RDP-Tcp** connection and click **Properties**.

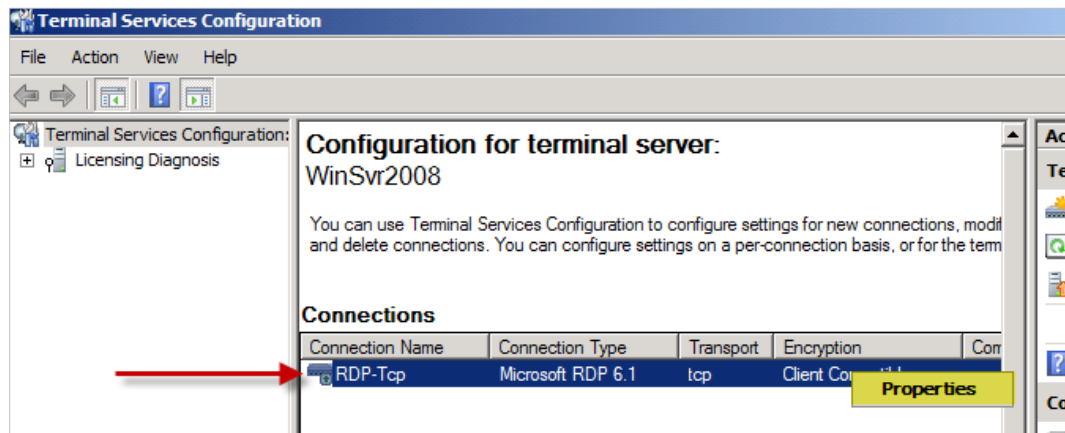


Figure 30 - Configuring TS Server Options

- ▶ **General Tab** – allows you to configure the following:
 - ▶ **Security Layer** – these settings allow you to configure either **RDP Security Layer**, which allows only native RDP encryption between clients; **Negotiate**, which negotiates the highest supported security between clients; or **SSL (TLS 1.0)** only, which is the most secure.
 - ▶ **Encryption level** – these settings allow you to configure either **Low**, which all communication from the client is protected by the maximum key strength of the client; **Client Compatible**, which all communication is protected by the maximum key strength of the client; **High**, which all communication is protected by the maximum key strength of the server; or **FIPS Compliant**, which all communication is protected by the Federal Information Processing Standard 140-1 encryption methods.
- ▶ **Log on Settings Tab** – allows you to force users to enter a password, use client-provided log on information, or use administrator provided user and password information.
- ▶ **Sessions Tab** – allows you to configure session limits.
 - **End a disconnected session** – provides the ability to set a time limit before disconnecting users who are still logged on, but not connected to a Terminal Server.
 - **Active session limit** – allows you to set a time limit on the entire session.
 - **When session limit is reached or connection is broken** – allows you to either **Disconnect from session** or **End session**.

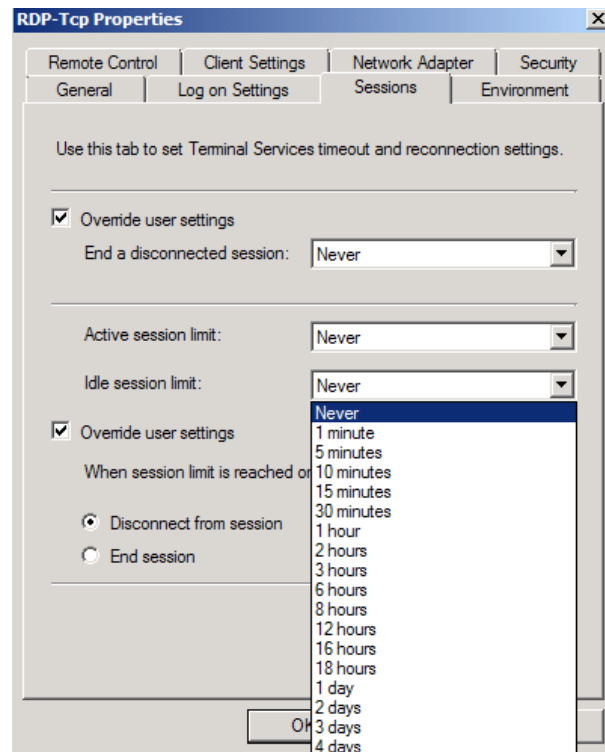


Figure 31 - Session Tab Properties

- ▶ **Environment Tab** – provides the ability to configure how an initial program will be launched in Terminal Services session.
- ▶ **Remote Control Tab** – provides control over interactions with remote user sessions.
- ▶ **Client Settings Tab** – this tab provides control over options like Color Depth and disabling redirection for the following programs or services: Drive, Windows Printer, LPT Port, COM Port, Clipboard, Audio, Supported Plug and Play Devices, and Default to main client printer.
- ▶ **Network Adapter Tab** – provides configuration options for the maximum number of connections.
- ▶ **Security Tab** – allows you to configure users and groups with the following permission sets: Full Control, User Access, Guest Access, and Special permissions.

Configuring Terminal Services Client Connections

Using the RDP client, you have granular control over client connections to terminal servers. These settings include, but are not limited to, display, keyboard, mouse, and local resource settings. RDP settings can be configured manually or through Group Policy.

To configure Terminal Services client connections, perform the following:

Navigate to **Start > All Programs > Accessories > Remote Desktop Connection** and click **Options**.

- **General Tab** – allows you to enter the name of the remote computer and your logon username.
- **Display Tab** – provides options to adjust your remote desktop screen size and color.
- **Local Resources Tab** – gives control over the use of the remote computer's sound, the remote computers keyboard, and local devices and resources. In other words, you can use your local hard drive in your remote session.
- **Programs Tab** – allows you to start programs on connection.
- **Experience Tab** – allows you to choose your connection speed. It also allows the following: desktop background, font smoothing, desktop composition, show contents of window while dragging, menu and window animation, themes and bitmap caching.
- **Advanced Tab** – provides TS Gateway Settings configuration options (see the Configuring Terminal Services Gateway section for more detailed information). It also enables you to verify that you are connecting to the intended computer. You are provided three options:
 1. **Connect and don't warn me** – allows a connection regardless if the remote connection can verify the remote computer.
 2. **Warn me** – gives a warning along with the option of continuing or not.
 3. **Do not connect** – will not allow a remote desktop connection if it cannot verify the remote computer.

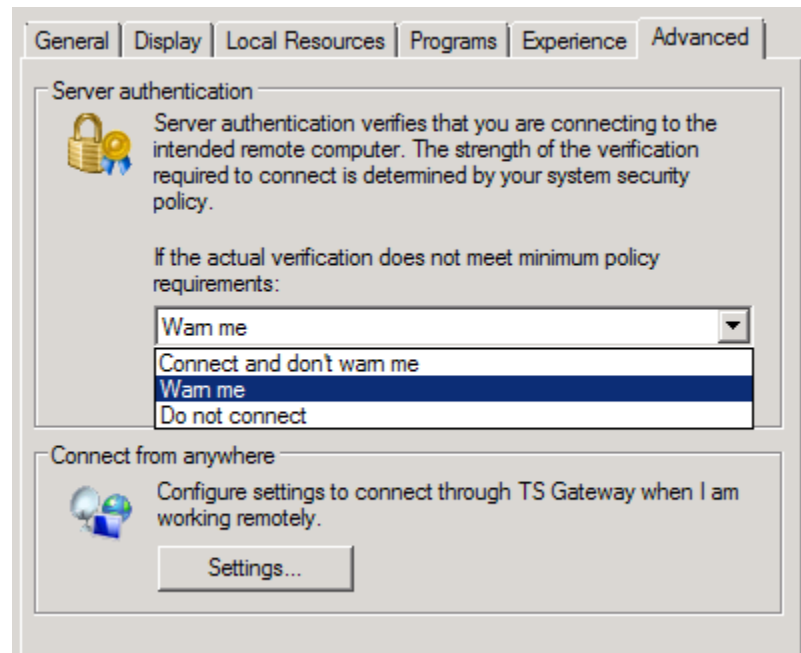


Figure 32 - RDP Advanced Properties

Configuring a Terminal Services Gateway

The TS Gateway service enables users, with proper credentials, to access to internal resources from computers over the internet. TS Gateway uses RDP over HTTPS to encrypt and secure the traffic between the computer connected to the Internet and the resources on the internal company network. Before you begin configuring the TS Gateway service, you must meet the following conditions:

- You must be a member of the local administrators group.
- You must request and install an SSL certificate.
- You must be running at least Windows Server 2008.

To further control access to internal resources, the TS Gateway Service uses two authorization policies:

- **Terminal Services Connection Authorization Policies (TS CAPs)** – allows you to specify which security groups and computers can access the TS Gateway server.
- **Terminal Services Resource Authorization Policies (TS RAPs)** – allows you to specify what resources authenticated users can connect to through a TS Gateway server.

Note that you can use the Group Policy Management Console to configure TS Gateway setting through using the following three options:

- **Set the TS Gateway Server Authentication Method** – allows you to select an authentication method for clients connecting to resources on the internal company network.
- **Enable Connections Through TS Gateway** – allows you to specify that clients use TS Gateway servers listed in the TS Gateway Server Address configuration.
- **Set the TS Gateway Server Address** – allows you to specify TS Gateway servers that clients can connect to for access to resources on the internal company network.

To configure Terminal Services Gateway, you must perform the following steps: install the Terminal Services Gateway Service; request and configure a certificate for the Terminal Services Gateway server; configure a Terminal Services Gateway CAP and a Terminal Services Gateway RAP; and configure the Remote Desktop Client.

Install the Terminal Services Gateway Service

It is recommended to place the TS Gateway server behind an Edge device, an Internet Security and Acceleration (ISA) server. Since users have to authenticate, placing the TS Gateway server in a DMZ is not recommended.

To install the TS Gateway service, perform the following: Navigate to **Start > Administrative Tools > Server Manager**.

1. In the right pane, under **Roles Summary**, click **Terminal Services**.
2. In the right pane, under **Roles Services**, click **Add Role Services**.
3. On the **Select Role Services** page, select **TS Gateway**.
4. On the **Add role services and features required for TS Gateway** page, click **Add Required Role Services**, and then click **Next**.

5. On the **Choose a Server Authentication Certificate for SSL Encryption** page, you have three options:
 - ▶ **Choose an existing certificate for SSL encryption** – this setting gives you the ability to install an existing certificate issued from a third-party or an internal certificate authority (CA).
 - ▶ **Create a self-signed certificate for SSL encryption** – this setting creates a self-signed certificate for the TS Gateway server. The certificate will need to be installed on the Trusted Root Certification Authorities store on client computers.
 - ▶ **Choose a certificate for SSL encryption later** – this allows you to install or import the certificate later. In order for clients to connect to a TS Gateway server, a certificate must be installed.
6. Select **Choose a certificate for SSL encryption later**, and then click **Next**.
7. On the **Create Authorization Policies for TS Gateway** page, you have two options:
 - ▶ **Now** – this setting allows you to configure a connection authorization policy (TS CAP) for the TS Gateway server.
 - ▶ **Later** – this setting allows you to create authorization policies later after installation.
8. Select **Later**, and then click **Next**.
9. On the **Select Role Services** page, verify that **Network Policy Server** is checked, and then click **Next**.
10. On the **Web Server (IIS)** page, click **Next**.
11. On the **Select Role Services** page, keep the default selections and click **Next**.
12. On the **Confirm Installation Selections** page, review the summary and click **Install**.
13. On the **Installation Result** page, click **Close**.

Request a certificate for a Terminal Services Gateway server

To request a certificate for a TS Gateway server, perform the following: Navigate to **Start > Administrative Tools > Internet Information Services (IIS) Manager**.

1. In the left pane, click the TS Gateway server.
2. In the middle pane, double click **Server Certificates**.

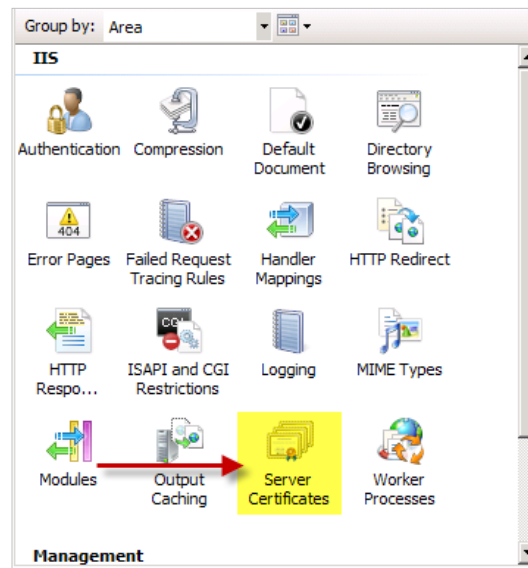


Figure 33 - Requesting Server Certificates for a TS Gateway

3. In the right pane, click **Create Domain Certificate**.
4. On the **Distinguished Name Properties** page, enter the required information. The **Common name** field is the most important of them all. Clients will use this name to access the TS Gateway server.

 A screenshot of the 'Create Certificate' wizard, specifically the 'Distinguished Name Properties' page. The page has a blue header with the text 'Create Certificate' and a sub-header 'Distinguished Name Properties' with a certificate icon. Below the sub-header is a grey box containing the text: 'Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.' Below this text are several input fields:

Common name:	<input type="text" value="TSGateway.trainingdomain.com"/>
Organization:	<input type="text" value="IT"/>
Organizational unit:	<input type="text" value="Hampton"/>
City/locality:	<input type="text" value="Hampton"/>
State/province:	<input type="text" value="VA"/>
Country/region:	<input type="text" value="US"/>

Figure 34 - Distinguished Name Properties

5. Click **Next**.
6. On the **Online Certification Authority** page, specify an online Certificate Authority and a Friendly name.
7. Click **Finish**.

Install a certificate on a Terminal Services Gateway server

To install a certificate on TS Gateway server, perform the following:

- Navigate to **Start > Terminal Services > TS Gateway Manager**.
 1. In the left pane, click the name of the TS Gateway server.
 2. In the middle pane under the **TS Gateway Server Status** section, click **View or Modify Certificate**.

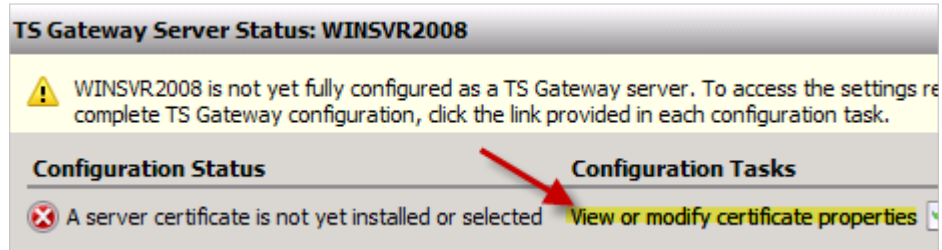


Figure 35 - Installing a Certificate on a TS Gateway

3. Choose **Select an existing certificate for SSL encryption**, and then click **Browse Certificates**.
4. On the **Install Certificate** page, select the appropriate certificate and click **Install**.

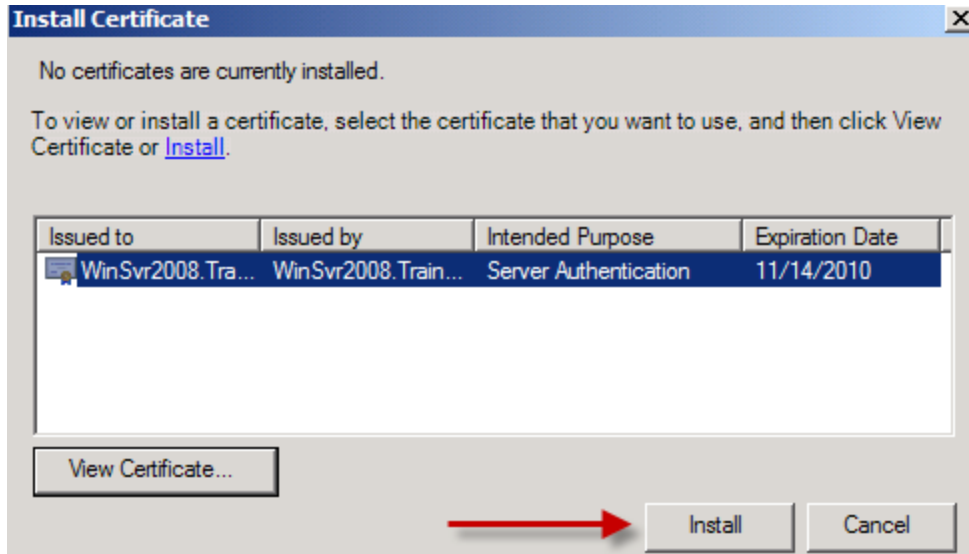


Figure 36 - Installing the Certificate

5. Click **OK**.

Configure a TS Gateway CAP and a TS Gateway RAP

To configure a TS Gateway Connection Authorization Policy (CAP) and a TS Gateway Resource Authorization Policy (RAP), perform the following: Navigate to **Start > Terminal Services > TS Gateway Manager**.

1. In the left pane, expand the name of the TS Gateway server.
2. Right-click the **Policies** folder and click **Create New Authorization Policies**.

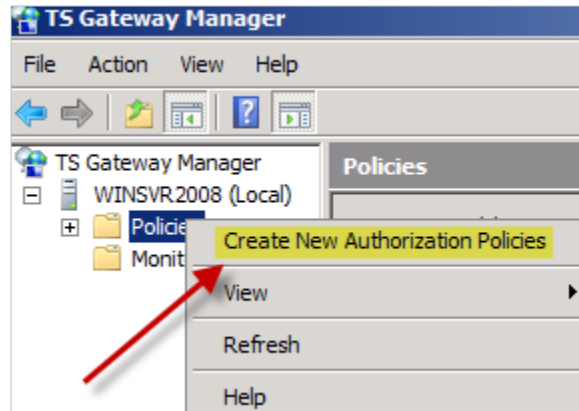


Figure 37 - Creating New Authorization Policies

3. On the **Create Authorization Policies for TS Gateway** page, select **Create a TS CAP and a RAP** and click **Next**.
4. On the **Create a TS CAP for TS Gateway** page, enter a name for the TS CAP, and then click **Next**.
5. On the **Create a TS CAP for TS Gateway** page under the **Requirements** section, select **Password** for one of the supported Windows authentication methods, and then add the Domain Users group as it will be associated with this TS CAP. You are also given the option to configure computers group membership, but we will leave this option blank. Click **Next**.

Create a TS CAP for TS Gateway

Specify at least one supported Windows authentication method. If you select both methods, users that use either method will be allowed to connect.

Password Smartcard

Add the user groups that will be associated with this TS CAP. Users who are members of these groups can connect to this TS Gateway server.

User group membership (required):

TRAININGDOMAIN\Domain Users

Optionally, you can add [computer groups](#) that will be associated with this TS CAP. Client computers that are members of these groups can connect to this TS Gateway server.

Client computer group membership (optional):

Figure 38 - Fulfilling TS CAP Requirements

6. On the **Create a TS CAP for TS Gateway** page under the **Device Redirection** section, you have three options:
 - ▶ **Enable device redirection for all client devices.**
 - ▶ **Disable device redirection for all client devices except for smart cards.**
 - ▶ **Disable device redirection for the following devices types:** drives, clipboard, printers, serial ports, and supported Plug and Play devices.
7. Select **Enable device redirection for all client devices**, and then click **Next**.
8. Review the TS CAP summary and click **Next**.
9. On the **Create a TS RAP for TS Gateway** page, enter a name for the TS RAP policy. Click **Next**.
10. On the **Create a TS RAP for TS Gateway** page under the **User Groups** section, add the Domain Users group as it will be associated with this TS RAP. Members of the Domain Users group will be able to access resources via the TS Gateway. Click **Next**.

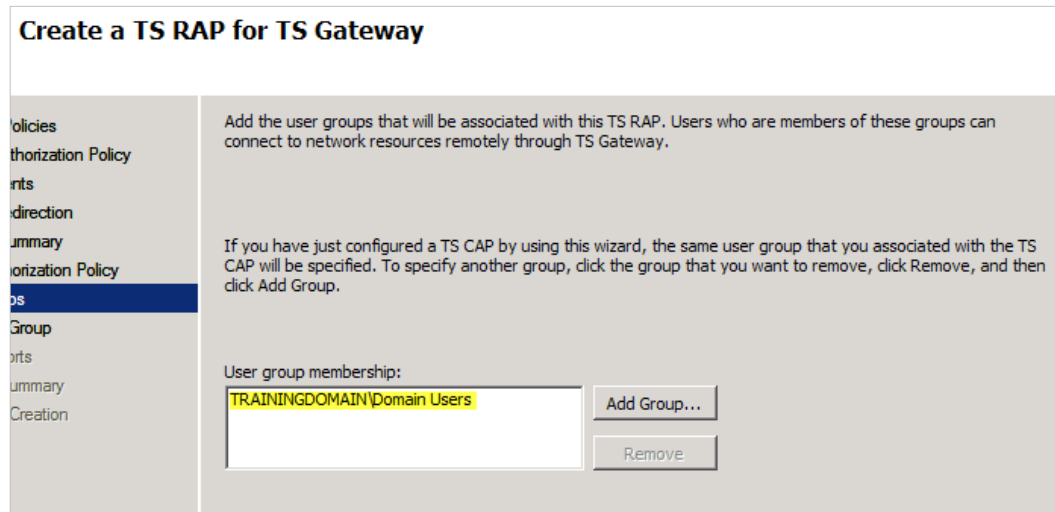


Figure 39 - Setting User Group Membership

11. On the **Create a TS RAP for TS Gateway** page under the **Computer Group** section, specify Terminal Servers users can connect to via the TS Gateway. You have three options:
 - ▶ **An existing Active Directory security group.**
 - ▶ **An existing TS Gateway-managed computer group, or create a new one.**
 - ▶ **Allow users to connect to any network resource (computer).**
12. Select **Allow users to connect to any network resource**, and then click **Next**.
13. On the **Create a TS RAP for TS Gateway** page under the **Allowed Ports** section, specify the port number that clients will connect through. You have three options:
 - ▶ **Allow connections only through TCP port 3389.**
 - ▶ **Allow connections through these ports** (you must specify port numbers).
 - ▶ **Allow connections through any port.**
14. Select **Allow connections only through TCP port 3389**, and then click **Next**.
15. Review the summary and click **Finish**.
16. On the Create Policies for TS Gateway, it confirms both policies were created successfully. Click **Close**.

Configure a Remote Desktop Client to use a TS Gateway

Configuring RDP clients to use a TS Gateway server can be configured manually or through Group Policy.

To configure a RDP client to use a TS Gateway manually, perform the following:

- Navigate to **Start > All Programs > Accessories > Remote Desktop Connection**.
 1. In the **Remote Desktop Connections** dialog box, expand **Options** and click the **Advanced** tab.
 2. Verify **Warn me** is selected in the **Server authentication** section, and then click **Settings** in the **Connect from anywhere** section.

3. On the **Add role services and features required for TS Gateway** page, click **Add Required Role Services**, and then click **Next**.
4. On the **Web Server (IIS)** page, review the information and click **Next**.
5. In the **TS Gateway Server Settings** dialog box, select **Use these RD Gateway server settings** and type the TS Gateway server name. Note that “Automatically detect RD Gateway server” setting is dependent on Group Policy. For the **Logon method**, you have three options:

Remote Desktop Connection

Connection settings

Automatically detect RD Gateway server settings
 Use these RD Gateway server settings:
 Server name:
 Logon method:
 Bypass RD Gateway server for local addresses
 Do not use an RD Gateway server

Logon settings

User name: None specified

You will be asked for credentials when you connect to this RD Gateway server.

Use my RD Gateway credentials for the remote computer

Figure 40 - Configuring RDC to Use TS Gateway

- ▶ **Allow me to select later** – gives you the option to select a logon method when you connect.
 - ▶ **Ask for password (NTLM)** – prompts for a password.
 - ▶ **Smart card** – prompts for a smart card.
6. Select **Ask for password (NTLM)**. Note that the “Bypass RD Gateway server for local addresses” setting prevents local traffic from routing through TS Gateway if it is checked.
 7. Click **OK**, and then **Connect**.

Configuring Terminal Services RemoteApp

RemoteApp programs are applications that appear as if they are running locally on the client's computer, but are really running and using resources on a terminal server. The redirection of resources back to the terminal server is transparent to the end user. RemoteApp can be access and executed in multiple ways:

- You can access and execute a RemoteApp using the TS Web Access website.
- You can execute an RDP file (.rdp).
- You can execute an icon stored on your desktop via a Window Install (.msi) package.

Note that TS RemoteApp is installed along with the TS role service.

Deploy RemoteApp Programs through TS Web Access

To deploy RemoteApp programs through TS Web Access, you must add an application to the RemoteApp program, and install and configure the TS Web Access role service.

To add an application to the RemoteApp program, perform the following: Navigate to **Start > Administrative Tools > Terminal Services > TS RemoteApp Manager**.

1. From the actions menu, click **Add RemoteApp Programs**.
2. On the **Welcome to the RemoteApp Wizard** page, click **Next**.
3. On the **Choose programs to add to the RemoteApp Programs list** page, select the appropriate application(s) and click **Next**.

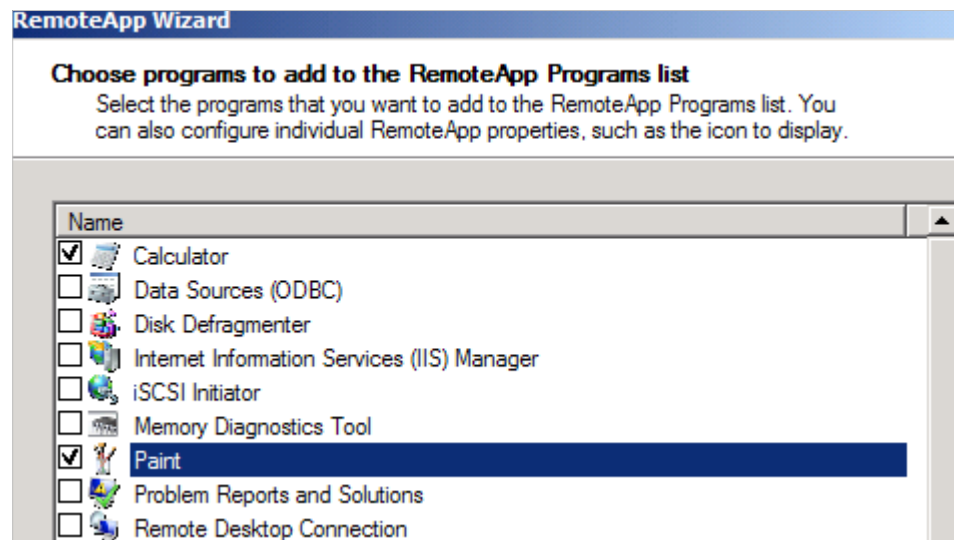


Figure 41 - Choosing RemoteApp Programs

4. Note that you should view the properties of the program and ensure **RemoteApp program is available through TS Web Access** is checked.
5. On the **Review Settings** page, click **Finish**.
6. Note that on the **RemoteApp Programs** list you will see the selected applications are enabled for TS Web Access.

To install and configure the TS Web Access role service, perform the following:
Navigate to **Start > Administrative Tools > Server Manager**.

1. In the right pane, under **Roles Summary**, click **Terminal Services**.
2. In the right pane, under **Roles Services**, click **Add Role Services**.
3. On the **Select Role Services** page, select **TS Web Access**.

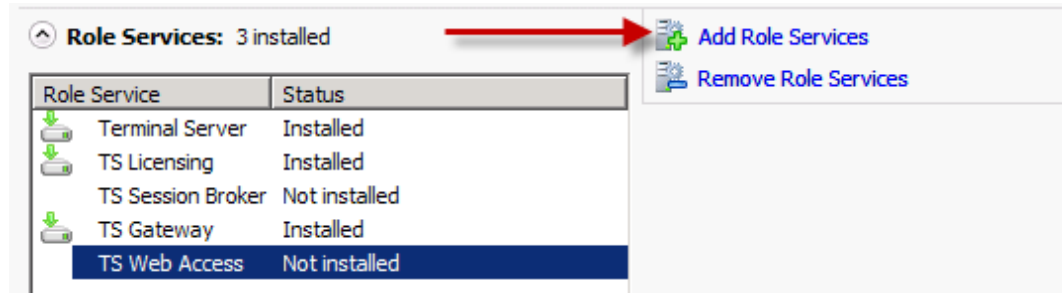


Figure 42 - Installing TS Web Access

4. On the **Select Role Services** page, keep the default selections and click **Next**.
5. On the **Confirm Installation Selections** page, review the summary and click **Install**.
6. On the **Installation Result** page, click **Close**.
7. If the TS server and TS Web Access server are on different computers, you must add the TS Web Access server to the TS Web Access security group on the TS server.

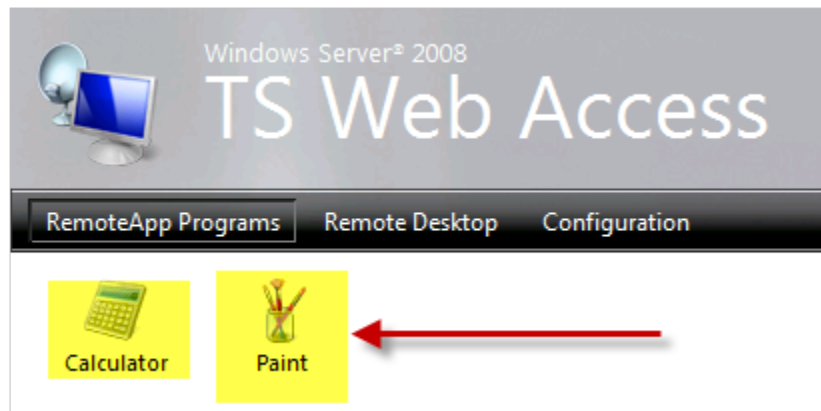


Figure 43 - TS Web Access Installed Programs

8. Now, test your TS Web Access by entering the following URL using Internet Explorer:
 - ▶ <http://YourServerName/ts>

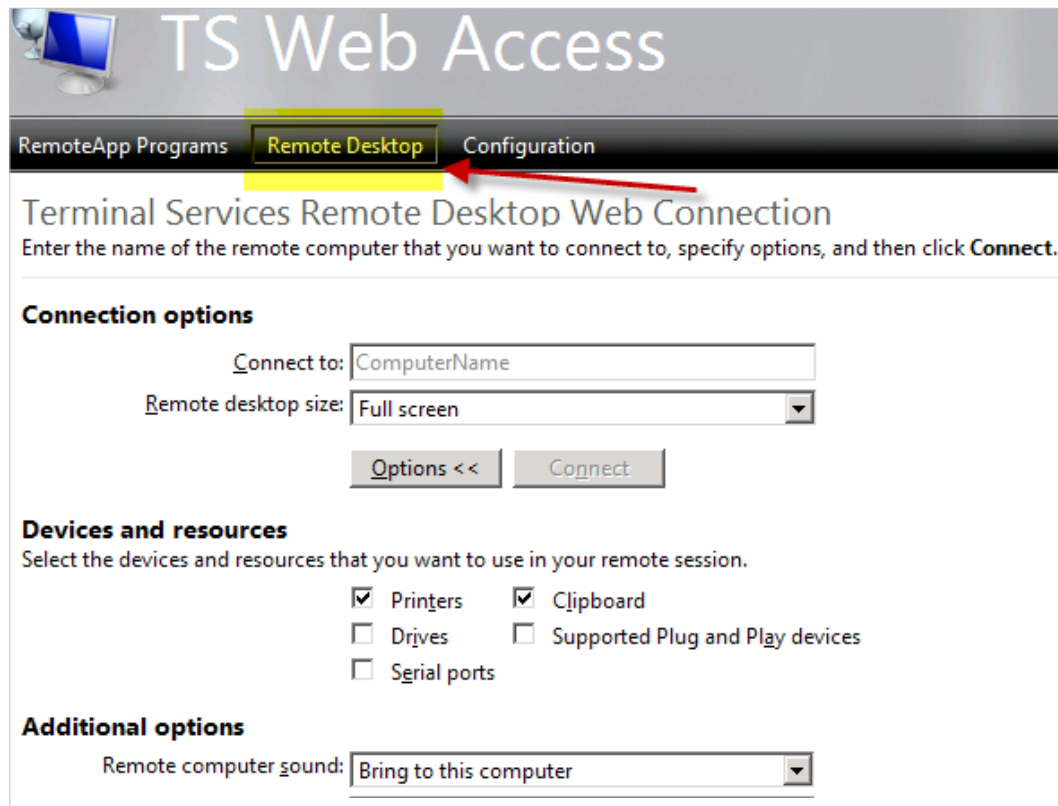


Figure 44 - TS Web Access Remote Desktop

- ▶ Note that you can establish Remote Desktop connections to Terminal Servers via the TS Web Access website by clicking the **Remote Desktop** button, as shown above, and entering a Terminal Server name.

In addition to the TS Web Access, you can deploy RemoteApp programs to users by distributing .msi packages to users and .rdp files. You can use the RemoteApp wizard to create and deploy any application in the RemoteApp programs list. To create an .rdp file, perform the following: Navigate to **Start > Administrative Tools > Terminal Services > TS RemoteApp Manager**.

1. In the **RemoteApps Programs** lists, click the programs for which you want to create .rdp files.
2. In the right pane, click **Create .rdp Files**.

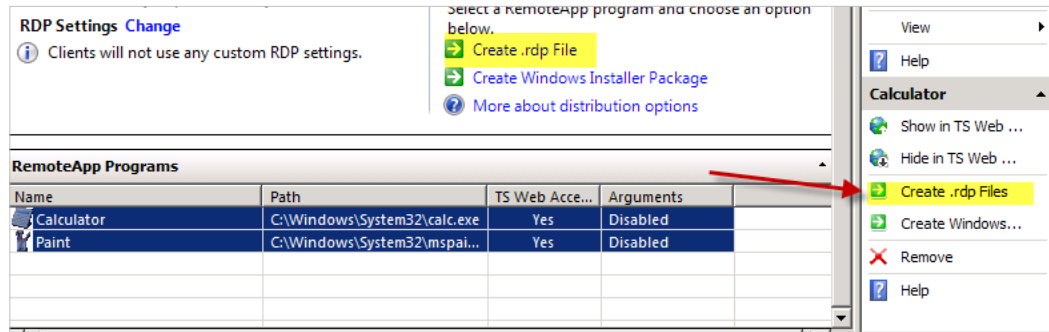


Figure 45 - Creating an RDP File

3. On the **Welcome to the RemoteApp** page, click **Next**.
4. On the Specify Package Settings page, you have four settings.

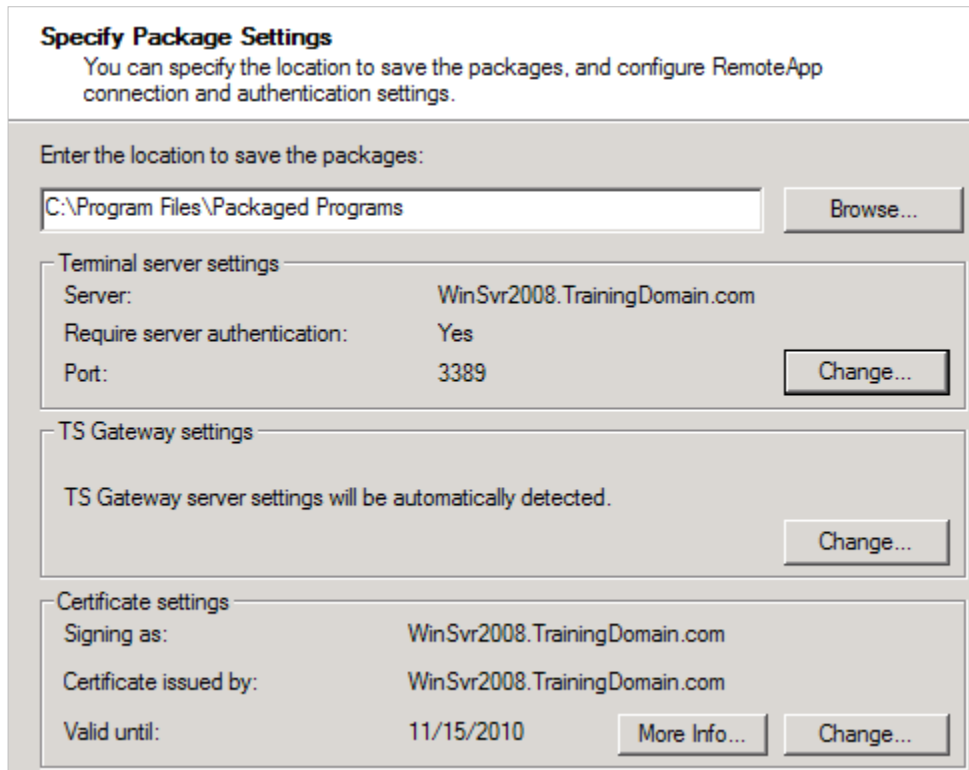


Figure 46 - Specify Package Settings

- ▶ In the **Enter the location to save the package** section, keep the default setting or click **Browse** to specify your own path.
- ▶ In the **Terminal server settings** section, keep the default port number or click **Change** to specify your own port number.
- ▶ In the **Gateway settings** section, keep the default setting.
- ▶ In **Certificate settings** section, click **Change** if you want to select a certificate and sign the application.

5. Click **Next**.
6. Review your settings and click **Finish**.
7. Your .rdp files are now ready for deployment.

Configuring Terminal Services Load Balancing

The TS Session Broker service enables session load balancing between terminal servers in a farm. In other words, new sessions are directed to terminal servers with the lowest number of connections. There is a two-step process when using the TS Session Broker to load balance a session.

- **DNS Round Robin** - This enables the DNS service to alternate between resource records that are returned to the clients.
 - ▶ Using the FARM server name, a user initiates a request using the RDP client.
 - ▶ The client queries a DNS server.
 - ▶ The client uses the first IP address in the list of addresses received from the DNS server. The client then contacts the terminal server.
- **Redirector Queries TS Broker Session server** - After the client contacts the terminal server, the terminal server acts as the redirector. The redirector queries the TS Broker Session database to decide to which terminal server the client should be directed.

To configure TS Session Broker Load Balancing, install the TS Session Broker role, populate the Session Directory Computer group, configure terminal server to join a farm, and then configure DNS.

Install a TS Session Broker

To install a TS Session Broker, perform the following:
Navigate to **Start > Administrative Tools > Server Manager**.

1. In the right pane, under **Roles Summary**, click **Terminal Services**.
2. In the right pane, under **Roles Services**, click **Add Role Services**.
3. On the **Select Role Services** page, select **TS Session Broker** and click **Next**.
4. On the **Confirm Installation Selections** page, review the summary and click **Install**.
5. On the **Installation Result** page, click **Close**.

Configure a TS Session Broker

To configure a TS Session Broker, perform the following: Navigate to **Start > Administrative Tools > Terminal Services Configuration**.

1. In the middle pane, under **Edit Settings**, right-click **Member of farm in TS Session Broker**, and click **Properties**.

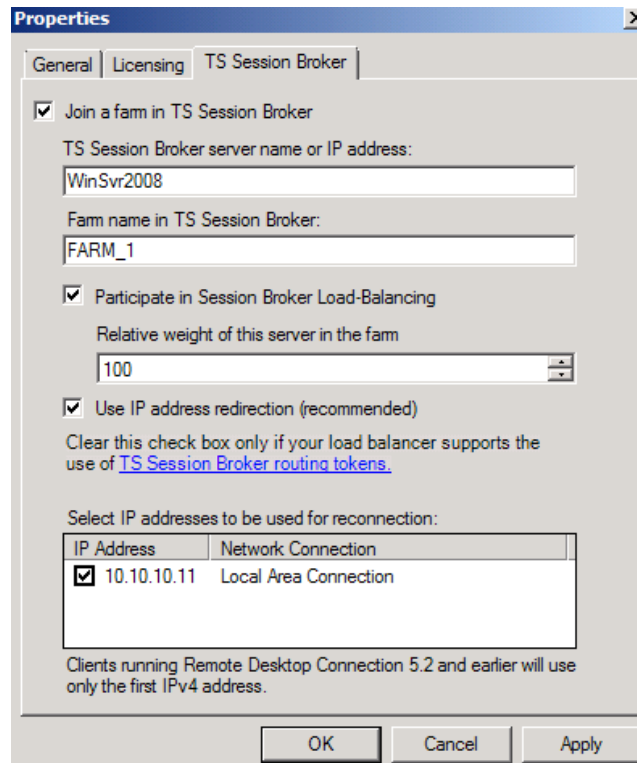


Figure 47 - TS Session Broker Properties

2. Select **Join a farm in TS Session Broker**.
3. In the **TS Session Broker server or IP** section, enter the name the server where you installed the TS Session Broker role service.
4. In the **Farm name in TS Session Broker** section, enter a farm name that you will use for all your Terminal Servers in the same farm.
5. Select **Participate in Session Broker Load-Balancing**.
6. In the **Relative weight of this server in the farm** section, enter your preferred relative weight. If the relative weight server_1 is 100 and the relative weight on server_2 is 400, then server_2 will take on 4 times the workload.
7. Select **Use IP address redirection**.
8. In the **Select IP addresses to be used for reconnection** box, check all IP participating addresses.

Note that you must configure DNS round robin for the TS Session Broker Load Balancing. Using the DNS Management MMC, you must map the IP address of each terminal server in the farm to the Terminal Services farm name. For example, create a host record for each server named "FARM_1."

Configuring and Monitoring Terminal Services Resources

Windows System Resource Manager (WSRM) enables an administrator to allocate resources to processes, applications, and services. For example, an administrator can control the amount of memory a particular application can be allotted.

Use the Windows System Resource Manager snap-in to configure WSRM. For terminal servers, there are two configurable resource-allocation policies:

- **Equal_Per_User** – divides resources equal among the logged on users.
- **Equal_Per_Session** – gives each user session an equal share of CPU resources.

Install Windows System Resource Manager

To install Windows System Resource Manager, perform the following:
Navigate to **Start > Administrative Tools > Server Manager**.

1. In the left pane, select **Features**.
2. In the **Features Summary** pane, click **Add Features**.

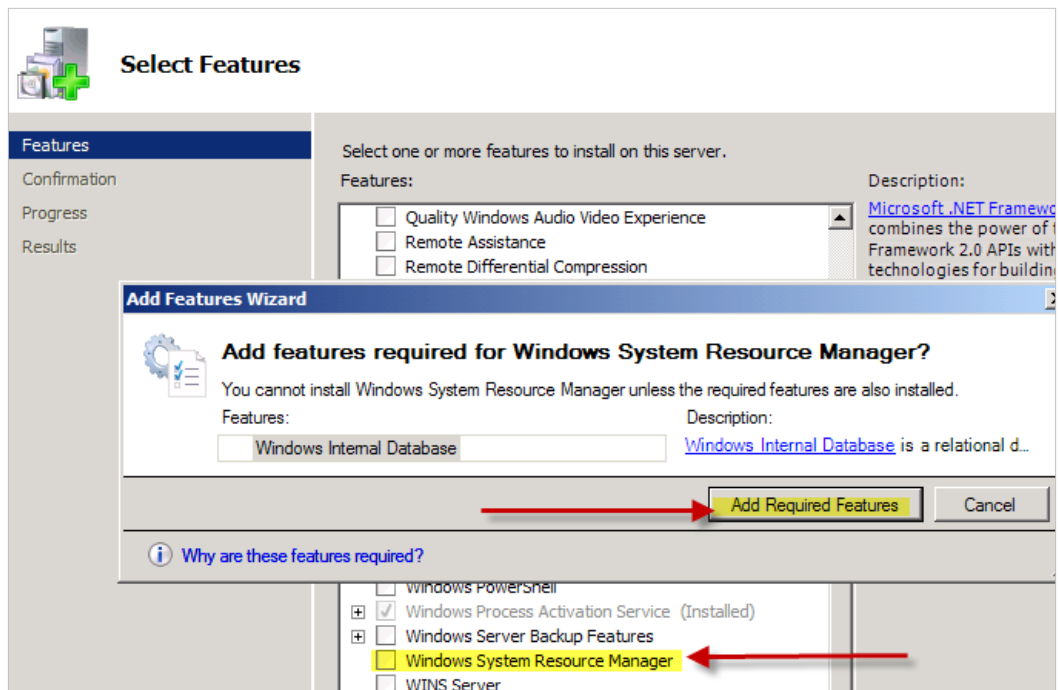


Figure 48 - Installing WSRM

3. On the **Select Features** page, select **Windows System Resource Manager**.
4. On the **Add features required for Windows System Resource Manager** page, click **Add Required Features** and then click **Next**.
5. On the **Confirm Installation Sections** page, click **Install**.
6. On the **Installation Results** page, click **Close**.

To configure the Equal-Per_Session resource-allocation policy, perform the following: Navigate to **Start > Administrative Tools > Windows System Resource Manager**.

1. Select **This computer** and click **Next**.
2. In the left pane, expand **Resource Allocation Policies**.

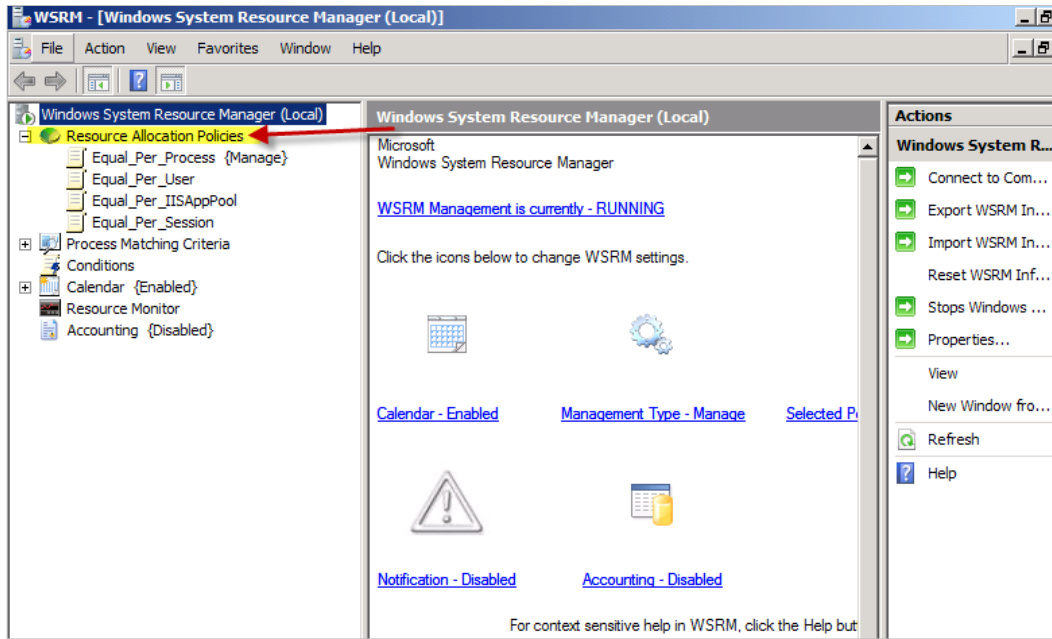


Figure 49 - Configuring Resource Allocation Policies

3. Right click **Equal_Per_Session**, and click **Set as Managing Policy**.
4. A warning box appears; click **OK**.

Configure Application Logging

WSRM logs accounting data about applications that are controlled by the managing policy and a policy that is set to profiling. The data is stored in a local or remote accounting database, or a SQL database. The information stored in the accounting data stores includes but is not limited to the following:

- Computer Name
- Process Name
- Domain
- User
- Session ID
- Thread Count
- Total CPU Time

To enable or disable Accounting, perform the following: Navigate to **Start > Administrative Tools > Windows System Resource Manager**. In the left pane, right click **Accounting** and click **Enable** or **Disable**.

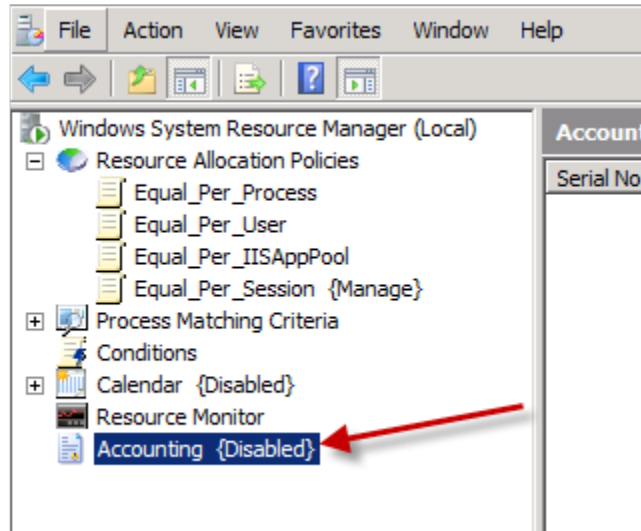


Figure 50 - Enabling or Disabling Accounting

As you can see, Windows Server 2008 offers granular control and monitoring capabilities over system resources.

Terminal Services Gets a Facelift in Windows Server 2008 R2

One of the most important changes to Terminal Services for candidates taking the 70-643 exam is in the area of naming. The server roles have all received new names in Windows Server 2008 R2. The following table provides the links from the old names to the new names:

Old Name	New Name
Terminal Services	Remote Desktop Services
Terminal Server	Remote Desktop Session Host (RD Session Host)
Terminal Services Licensing (TS Licensing)	Remote Desktop Licensing (RD Licensing)
Terminal Services Gateway (TS Gateway)	Remote Desktop Gateway (RD Gateway)
Terminal Services Session Broker (TS Session Broker)	Remote Desktop Connection Broker (RD Connection Broker)
Terminal Services Web Access (TS Web Access)	Remote Desktop Web Access (RD Web Access)

Several role services are also used by Remote Desktop Services (RDS) in Windows Server 2008 R2. These also have new names compared to the old names in earlier versions and the new names are listed in the following table:

Old Name	New Name
Terminal Services Manager	Remote Desktop Services Manager
Terminal Services Configuration	Remote Desktop Session Host Configuration
TS Gateway Manager	Remote Desktop Gateway Manager
TS Licensing Manager	Remote Desktop Licensing Manager
TS RemoteApp Manager	RemoteApp Manager

For the purposes of the exam, knowing these new names provides the primary set of new information you will need for RDS. However, you can learn more details about the new feature for remote application and desktop implementation here <http://technet.microsoft.com/en-us/library/dd560658%28WS.10%29.aspx>.

Domain 3: Configuring a Web Services Infrastructure

Manage Internet Information Services (IIS)

Internet Information Services (IIS) 7.0, a server role in Windows Server 2008, consists of several modules. These modules can be installed on-demand by administrators. In other words, administrators can granularly configure and include only what they need to support web applications. These modules include the following:

- **Common HTTP Features** – use the Common HTTP features to configure how the web server responds to requests. Custom error messages can also be created using this module.
- **Application Development** – provides the foundation for developing and hosting web applications. Technologies integrated in this module include but are not limit to ASP, ASP.NET, and CGI.
- **Health and Diagnostics** – gives the ability to monitor and manage the health of web servers, web sites, and web applications.
- **Security** – provides the ability to secure the web server by way of multiple authentication methods and authorizations. This module also offers the ability to reject and restrict requests based on user defined matches and originating IP spaces, respectively.
- **Performance** – integrates dynamic output caching capabilities of ASP.NET with static output caching included in IIS 6.0. It also improves bandwidth usage by the use of enhanced compression mechanisms.
- **Management** – provides a way to manage applications running IIS 7.0 via the user interface or command line.

Installing IIS 7.0 on Windows Server 2008

To install IIS 7.0, perform the following:

- Navigate to **Start > Administrative Tools > Server Manager**.
 1. On the **Roles Summary** page, click **Add Roles**.
 2. On the **Select Server Roles** page, select **Web Server (IIS)**.
 3. Click **Next**.
 4. On the **Select Role Services** page, select the role(s) to support your web application and click **Next**.

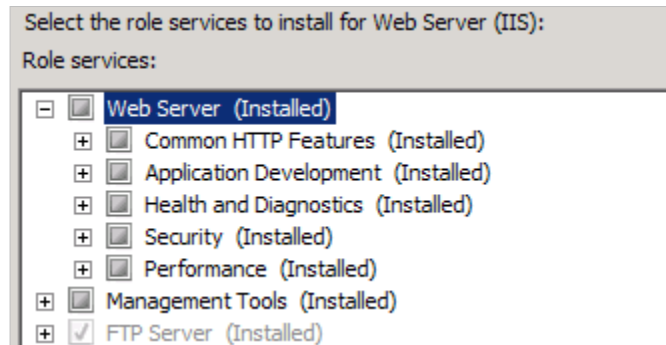


Figure 51 - Selecting Web Server Role Services

5. On the **Add role services required for ASP.NET** page, click **Add Required Role Services**.
6. On the **Confirm Installation Selections** page, review the summary and click **Install**.
7. On the **Installation Result** page, click **Close**.

Installing IIS 7.0 on Server Core

Installing IIS 7.0 on Server Core is not a huge task. You can use pkgmgr.exe on Server Core to perform a complete install. The following features are not available on Server Core:

- IIS-ASPNET
- IIS-NetFxExtensibility
- IIS-ManagementConsole
- IIS-ManagementService
- IIS-LegacySnapIn
- IIS-FTPManagement
- WAS-NetFxEnvironment
- WAS-ConfigurationAPI

To install IIS 7.0 on Server Core, type the following in the command-line window:

```
start /w pkgmgr /iu:IIS-WebServerRole;IIS-WebServer;IIS-CommonHttpFeatures;IIS-StaticContent;IIS-DefaultDocument;IIS-DirectoryBrowsing;IIS-HttpErrors;IIS-HttpRedirect;IIS-ApplicationDevelopment;IIS-ASP;IIS-CGI;IIS-ISAPIExtensions;IIS-ISAPIFilter;IIS-ServerSideIncludes;IIS-HealthAndDiagnostics;IIS-HttpLogging;IIS-LoggingLibraries;IIS-RequestMonitor;IIS-HttpTracing;IIS-CustomLogging;IIS-ODBCLogging;IIS-Security;IIS-BasicAuthentication;IIS-WindowsAuthentication;IIS-DigestAuthentication;IIS-ClientCertificateMappingAuthentication;IIS-IISCertificateMappingAuthentication;IIS-URLAuthorization;IIS-RequestFiltering;IIS-IPSecurity;IIS-Performance;IIS-HttpCompressionStatic;IIS-HttpCompressionDynamic;IIS-WebServerManagementTools;IIS-ManagementScriptingTools;IIS-IIS6ManagementCompatibility;IIS-Metabase;IIS-WMICompatibility;IIS-LegacyScripts;IIS-FTPPublishingService;IIS-FTPService;WAS-WindowsActivationService;WAS-ProcessModel
```

Configure IIS Delegation of Administrative Rights

An administrator's pet peeve is giving web site administrators and developers complete administrative control on Web servers. IIS 7.0 mitigates the need to unnecessarily elevate permissions allowing locking and unlocking of sections in the applicationHost.config file. This is called feature delegation. Permissions can be granted and controlled at the server level, site level, and folder level.

IIS 7.0 configuration settings are now centrally stored in the XML-based file named applicationHost.config. The applicationHost.config file contains features and components of IIS 7.0. Modifications to this file will affect IIS 7.0 globally. Settings in this file can be overridden by unlocking global settings by section. After unlocking the section, web site and web application owners can then override settings by modifying the web.config file located at the site and application level.

With feature delegation, administrators have the ability to delegate control over, http tracing for example, to site and application owners. The below applicationHost.config file shows how you can modify the **overrideModeDefault** property to **Allow** or **Deny** site and application owners the ability to override features in the web.config file.

```
-->
<configSections>
  <sectionGroup name="system.applicationHost">
    <section name="applicationPools" allowDefinition="AppHostOnly" overrideModeDefault="Deny" />
    <section name="configHistory" allowDefinition="AppHostOnly" overrideModeDefault="Deny" />
    <section name="customMetadata" allowDefinition="AppHostOnly" overrideModeDefault="Deny" />
    <section name="listenerAdapters" allowDefinition="AppHostOnly" overrideModeDefault="Deny" />
    <section name="log" allowDefinition="AppHostOnly" overrideModeDefault="Deny" />
    <section name="sites" allowDefinition="AppHostOnly" overrideModeDefault="Deny" />
    <section name="webLimits" allowDefinition="AppHostOnly" overrideModeDefault="Deny" />
  </sectionGroup>

  <sectionGroup name="system.webServer">
    <section name="asp" overrideModeDefault="Deny" />
    <section name="caching" overrideModeDefault="Allow" />
    <section name="cgi" overrideModeDefault="Deny" />
    <section name="defaultDocument" overrideModeDefault="Allow" />
    <section name="directoryBrowse" overrideModeDefault="Allow" />
    <section name="fastCgi" allowDefinition="AppHostOnly" overrideModeDefault="Deny" />
    <section name="globalModules" allowDefinition="AppHostOnly" overrideModeDefault="Deny" />
    <section name="handlers" overrideModeDefault="Deny" />
    <section name="httpCompression" allowDefinition="AppHostOnly" overrideModeDefault="Deny" />
    <section name="httpErrors" overrideModeDefault="Deny" />
    <section name="httpLogging" overrideModeDefault="Deny" />
    <section name="httpProtocol" overrideModeDefault="Allow" />
    <section name="httpRedirect" overrideModeDefault="Allow" />
    <section name="httpTracing" overrideModeDefault="Deny" />
    <section name="isapiFilters" allowDefinition="MachineToApplication" overrideModeDefault="Deny" />
  </sectionGroup>
</configSections>
```

Figure 52 - ApplicationHost.config File

Note that the web.config file is located at the root site level and application level. Remember that the lowest level, where the web.config resides, will apply the settings that were set to "Allow" in the applicationHost.config file.

The web.config file contains the settings and configurations for .NET web applications. This file controls security, module loading, session state, language, and compilation settings. A .NET web application inherits its base web.config from the machine's web.config located in %SystemRoot%\Microsoft.Net\Framework\v*.*.*\CONFIG folder. Below is a snippet from the machine's web.config file.

```
<compilation>
  <assemblies>
    <add assembly="mscorlib" />
    <add assembly="System, Version=2.0.0.0, Culture=neutral,
    <add assembly="System.Configuration, Version=2.0.0.0, Cu
    <add assembly="System.Web, Version=2.0.0.0, Culture=neutr
    <add assembly="System.Data, Version=2.0.0.0, Culture=neut
    <add assembly="System.Web.Services, Version=2.0.0.0, Cult
    <add assembly="System.Xml, Version=2.0.0.0, Culture=neutr
    <add assembly="System.Drawing, Version=2.0.0.0, Culture=r
    <add assembly="System.EnterpriseServices, Version=2.0.0.0
    <add assembly="System.Web.Mobile, version=2.0.0.0, Cultur
    <add assembly="*" />
  </assemblies>
  <buildProviders>
    <add extension=".aspx" type="System.Web.Compilation.Page
    <add extension=".ascx" type="System.Web.Compilation.UserC
```

Figure 53 - Web.config File

You can also enable sections in the applicationHost.config file to be overridden in IIS Manager Features Delegation page. To override sections used in the Features Delegation page, perform the following steps: Navigate to **Start > Administrative Tools > Internet Information Services (IIS) Manager**.

1. Click the web server name in the left pane.
2. In the middle pane, double click **Feature Delegation**.

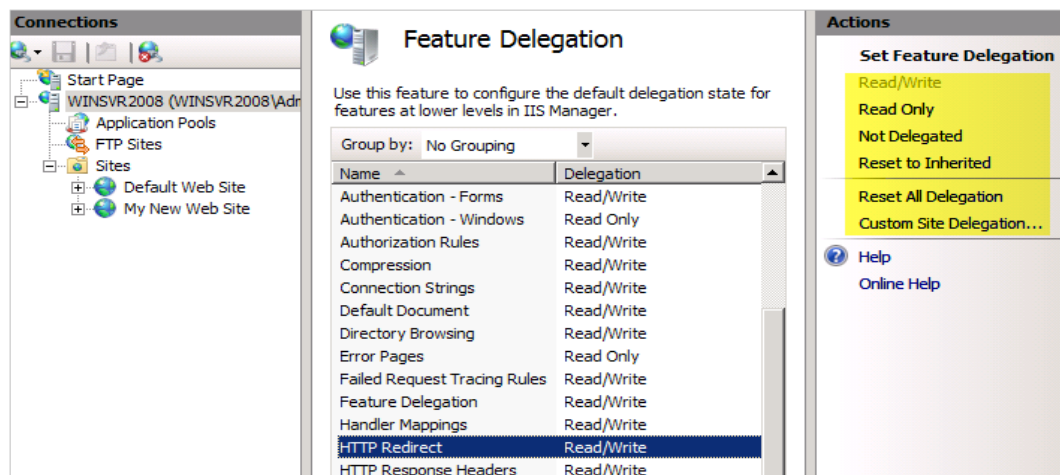


Figure 54 - Enabling Feature Delegation

There are six possible delegation settings:

- **Read/Write** – unlocks the targeted feature's configuration section in the configuration file. Configuration changes can be read from and modified in the web.config file.
- **Read Only** – locks the targeted feature's configuration section in the configuration file. Configuration changes cannot be modified in the web.config file.
- **Not Delegated** – locks the targeted feature's configuration section in the configuration file. Configuration changes cannot be read from or modified in the web.config file.
- **Reset to Inherited** – inherits the targeted feature's configuration settings from its parent.
- **Reset All Delegation** – affects all features. All configuration settings will be set in accordance with the parent settings.
- **Custom Site Delegation** – allows you to configure sections for an individual site or application.

Remote Management in IIS 7.0

As an added layer of security, remote management in IIS 7.0 must be enabled. This was not the case in IIS 6; remote management was always enabled. Configuration of remote administration can be configured through the Management Service page.

Who and what can be accessed is configured through the Management Service page. You, as web server administrator, can grant other administrators the ability to manage the web server. You can also grant users, non-administrators, the ability to manage delegated features of web sites and web application. Remember, access to these features was configured on the features delegation page.

To configure remote management in IIS 7.0, you must install the remote management role service first by performing the following: Navigate to **Start > Administrative Tools > Server Manager**.

1. In the **Server Manager Pane**, under the **Roles Summary** section, click **Web Server (IIS)**.
2. In the **Role Services** section, click **Add Role Services**.
3. On the **Select Role Services** page, select **Management Service** and click **Next**.
4. Confirm your installation settings and then click **Install**.

Once the remote management role service has been installed, you will see three new icons under the Management section in IIS Manger as shown below.

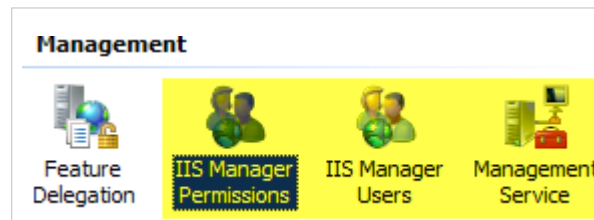


Figure 55 - IIS Manager Permissions

- **IIS Manager Users** – allows administrators to manage user accounts that can remotely manage sites and applications. Note that the configured IIS Manager user account is specific to IIS only.
- **IIS Manager Permissions** – allows administrators to manage IIS Manager users, Windows users, and Windows groups that can remotely manage sites and applications. You can grant users permissions to configure delegated features in any site and application.
- **Management Service** – allows administrators to remotely manage web servers that use IIS Manager. This feature also enables site and application owners to manage delegate features.

Remote management in previous versions of IIS was enabled by default. In IIS 7, you have to enable remote management and you have granular control over what sites administrators can access remotely. Perform the following steps to enable remote management: Navigate to **Start > Administrative Tools > Internet Information Services (IIS) Manager**.

1. Click the web server name in the left pane.

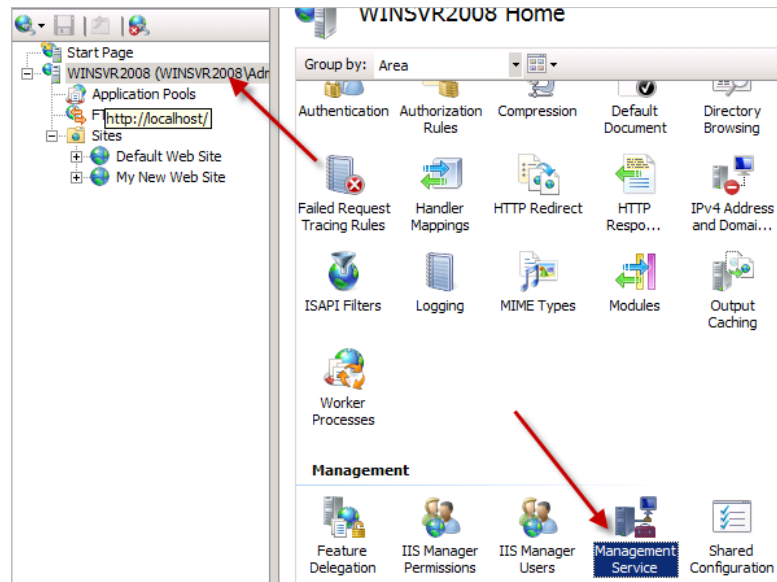


Figure 56 - Enabling Remote Management

2. In the middle pane, double click **Management Service**.

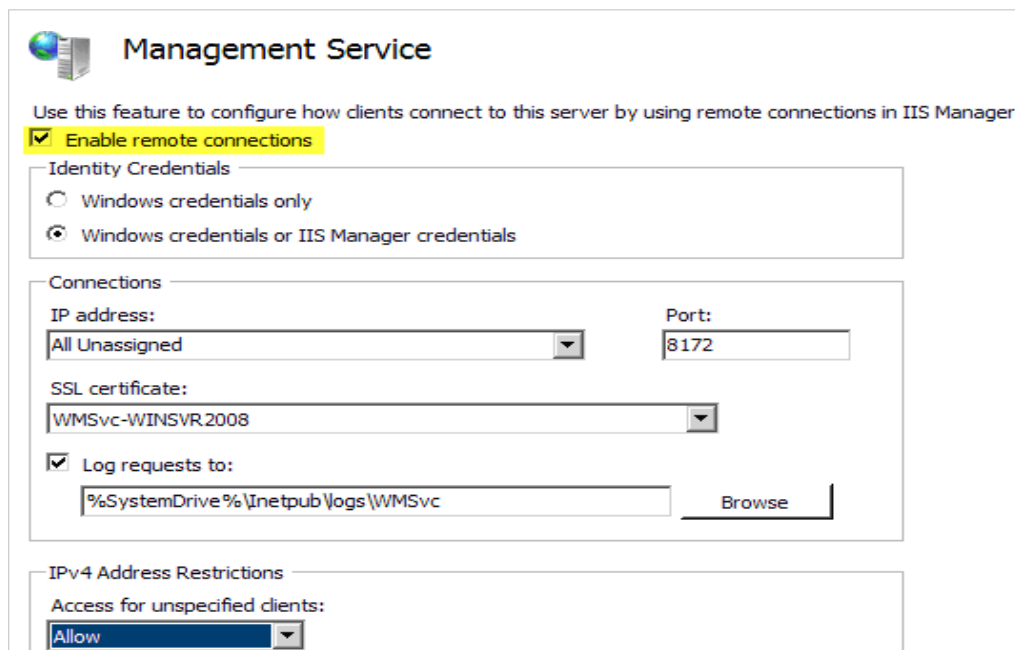


Figure 57 - Configuring IIS Remote Management

Note: before configuring remote management, you must stop the “**Management Service**” service first.

3. Ensure that **Enable remote connections** is checked.
4. Under the **Identity Credentials** section, you have two options:
 - ▶ **Windows credentials only** – select this option for users with Windows domain accounts.
 - ▶ **Windows credentials or IIS Manager credentials** – select this option for users with Windows domain accounts and IIS Manager accounts.
5. Under the **Connections** section, you have the option of selecting an IPv4 or IPv6 address; you have the options of typing a port number on which you want your server to listen; you have the option selecting an SSL certificate in order to secure communications; and you have the option to enable and log requests to the file system.
6. Under the **IPv4 Address Restrictions** section, you have the option of allowing or denying client remote access to the server.
7. In the right pane, click **Apply** and restart the “**Management Service**” service.

IIS Configuration Backup

IIS 7.0 disaster recovery can be performed using the APPCMD command-line tool.

- **Appcmd add backup “Name of Backup”** – this command creates a new configuration backup. After the backup is complete the following files are copied to the Windows\System32\inetsrv\Backup directory:
 - ▶ Administration.config
 - ▶ applicationHost.config
 - ▶ MBSchema.xml
 - ▶ MetaBase.xml
 - ▶ Redirection.config
- **Appcmd restore backup “Name of Backup”** – this command restores the configuration backup named “Name of Backup” to the server.
- **Appcmd delete backup “Name of Backup”** – this command removes the configuration backup named “Name of Backup” from the server.
- **Appcmd list backup** – this command lists all backups on the server.

Configure IIS Logging

IIS logging is a component of the Health and Diagnostic module. This module enables the ability to monitor and manage the health of web servers, web sites, and web applications. The logging feature page allows you to configure how IIS logs http requests made to the web server. Below is an example of a W3SVC log file locating in the %systemdrive%\inetpub\logfiles folder:

```
#Software: Microsoft Internet Information Services 7.0
#Version: 1.0
#Date: 2009-11-30 00:42:01
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent)
2009-11-30 00:42:01 :::1 GET /ping.axd - 8172 - :::1 Mozilla/4.0+(compatible;+win32;+winHttp.w
#Software: Microsoft Internet Information Services 7.0
#Version: 1.0
#Date: 2009-11-30 01:09:17
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent)
2009-11-30 01:09:17 :::1 GET /ping.axd - 8172 - :::1 Mozilla/4.0+(compatible;+win32;+winHttp.w
2009-11-30 01:14:17 :::1 GET /ping.axd - 8172 - :::1 Mozilla/4.0+(compatible;+win32;+winHttp.w
2009-11-30 01:19:17 :::1 GET /ping.axd - 8172 - :::1 Mozilla/4.0+(compatible;+win32;+winHttp.w
2009-11-30 01:24:17 :::1 GET /ping.axd - 8172 - :::1 Mozilla/4.0+(compatible;+win32;+winHttp.w
2009-11-30 01:29:17 :::1 GET /ping.axd - 8172 - :::1 Mozilla/4.0+(compatible;+win32;+winHttp.w
2009-11-30 01:34:17 :::1 GET /ping.axd - 8172 - :::1 Mozilla/4.0+(compatible;+win32;+winHttp.w
2009-11-30 01:39:17 :::1 GET /ping.axd - 8172 - :::1 Mozilla/4.0+(compatible;+win32;+winHttp.w
2009-11-30 01:44:17 :::1 GET /ping.axd - 8172 - :::1 Mozilla/4.0+(compatible;+win32;+winHttp.w
2009-11-30 01:49:17 :::1 GET /ping.axd - 8172 - :::1 Mozilla/4.0+(compatible;+win32;+winHttp.w
2009-11-30 01:54:17 :::1 GET /ping.axd - 8172 - :::1 Mozilla/4.0+(compatible;+win32;+winHttp.w
2009-11-30 01:59:17 :::1 GET /ping.axd - 8172 - :::1 Mozilla/4.0+(compatible;+win32;+winHttp.w
2009-11-30 02:04:17 :::1 GET /ping.axd - 8172 - :::1 Mozilla/4.0+(compatible;+win32;+winHttp.w
2009-11-30 02:09:17 :::1 GET /ping.axd - 8172 - :::1 Mozilla/4.0+(compatible;+win32;+winHttp.w
2009-11-30 02:14:17 :::1 GET /ping.axd - 8172 - :::1 Mozilla/4.0+(compatible;+win32;+winHttp.w
2009-11-30 02:19:17 :::1 GET /ping.axd - 8172 - :::1 Mozilla/4.0+(compatible;+win32;+winHttp.w
```

Figure 58 - W3SVC Log File

IIS 7.0 uses the following log file formats:

- **Binary** – the binary format saves on memory and CPU utilization. This format is typically used by large Internet Service Providers (ISPs).
- **W3C** – WSC uses IIS to log information about all sites on the web server.
- **IIS** – IIS is the Microsoft native IIS log file format.
- **NCSA** – IIS uses the National Center for Supercomputing Applications (NCSA) format to log information about sites. The NCSA format contains the following fields:
 - ▶ Remote host address
 - ▶ Remote log name
 - ▶ User name
 - ▶ Date, time, and UTC offset
 - ▶ Request and protocol version
 - ▶ Service status code
 - ▶ Bytes sent
- **Custom** – this format configures IIS to use a custom format from a third-party vendor.

To configure IIS logging, perform the following: Navigate to **Start > Administrative Tools > Internet Information Services (IIS) Manager**.

1. Click the web server name in the left pane.

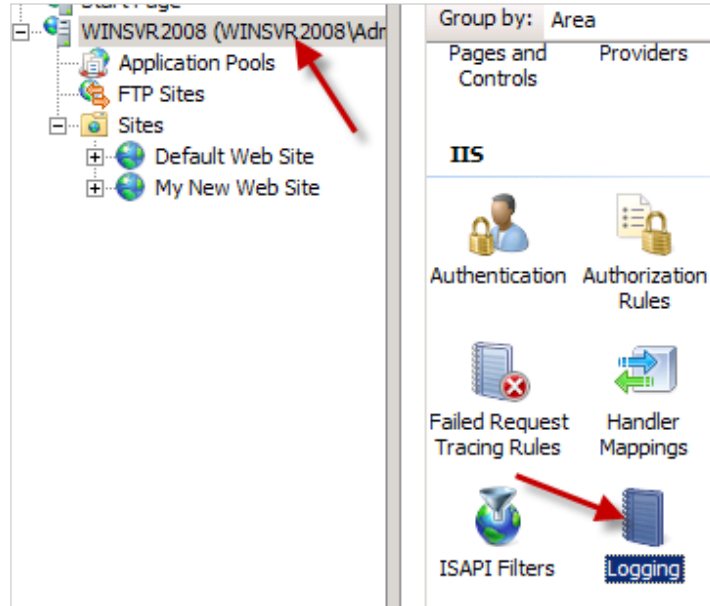


Figure 59 - Configuring IIS Logging

2. In the middle pane, double click **Logging**.

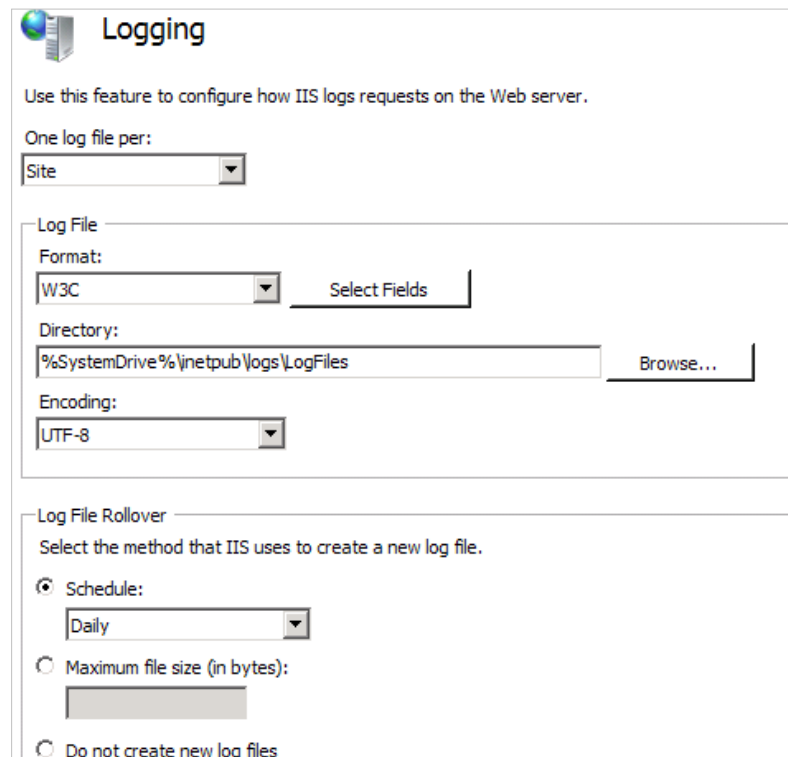


Figure 60 - IIS Logging

On the logging configuration page, you can specify one log file per site or server. You also have the option of configuring the log file format to IIS, NCSA, W3C, or Custom. Further down the logging configuration page, it enables you to select a method by which IIS creates new log files.

Health and Diagnostics

IIS 7.0 provides the ability to manage and monitor the health of web servers, sites, and applications. The Health and Diagnostics module contains the following features:

- **HTTP Logging** – writes web site activity to the appropriate log file store on the file system.
- **Logging Tools** – provides a way to manage web server logs.
- **Request Monitor** – provides a way for administrators to monitor http requests in a worker process. This feature is especially helpful when a worker process has become slow or unresponsive.
- **Tracing** – enables administrators to take a more granular approach by configuring their own error conditions. This feature will only log the trace if it meets the user-defined error condition.
- **Custom Logging** – allows administrators to create their own logging module and format.
- **ODBC Logging** – supports logging web server activities to an ODBC database.

Tracing Feature

Before you add a Failed Request Tracing Rule, you will need to enable Failed Request Tracing at the site level, application level, or directory level. For example, the tracing feature should be enabled if you want IIS to log failed attempts to display content from a site or application.

To enable Failed Request Tracing, perform the following:

Navigate to **Start > Administrative Tools > Internet Information Services (IIS) Manager**.

1. Click the web site name in the left pane.

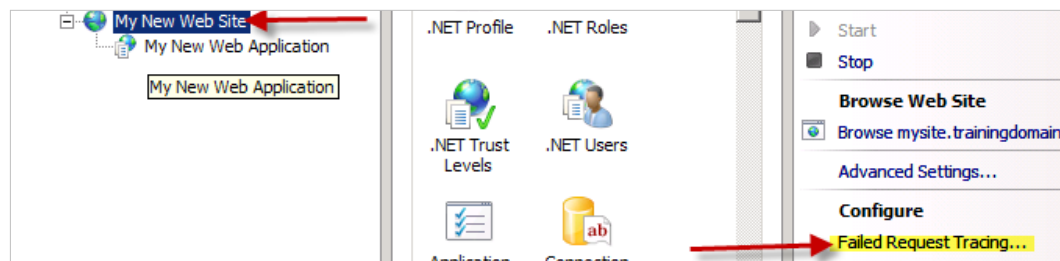


Figure 61 - Enabling Failed Request Tracing

2. In the right pane, click **Failed Request Tracing**.
3. Ensure **Enable** is checked.
4. Keep the default or change the **Directory** path and specify the **Maximum number of trace files**.
5. Click **OK**.

After Failed Request Tracing has been enabled for a site or multiple sites, add a Failed Request Tracing Rule by performing the following steps: Navigate to **Start > Administrative Tools > Internet Information Services (IIS) Manager**.

1. In the left pane, click the site node on which to enable tracing and double click the **Failed Request Tracing Rule** icon in the middle pane.
2. Within the Failed Request Tracing Rules window, right click and click **Add**.

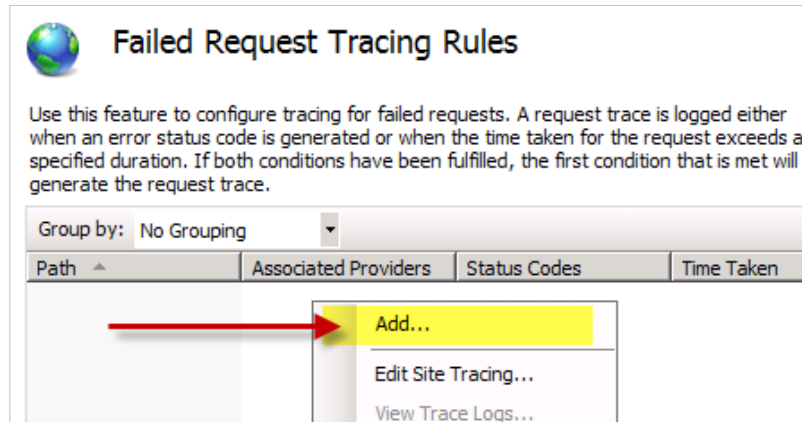


Figure 62 - Adding Failed Tracing Rules

3. In the **Specify Content to Trace** dialog box, select the content type and click **Next**.
4. In the **Define Trace Conditions** dialog box, select one or more the following rules:

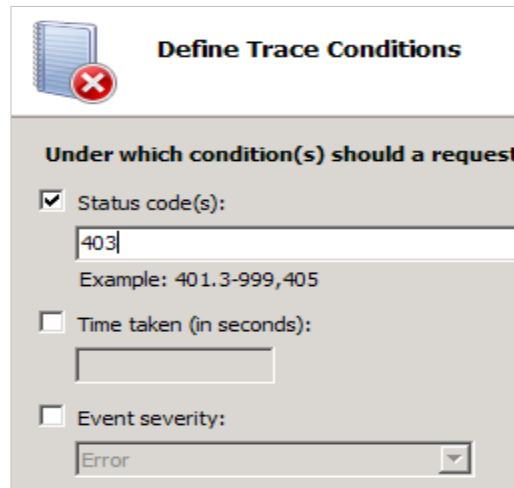


Figure 63 - Defining Trace Conditions

- ▶ **Status code(s)** – allows you to enter one or more status codes that you want to trace.
- ▶ **Time taken (in seconds)** – allows you to enter the amount of time you think a request should take.
- ▶ **Event severity** – allows you to select a severity code of Error, Critical Error, or Warning.

5. Click **Next**.
6. In the **Select Trace Providers** dialog box, under **Providers** select one or more of the following trace providers:

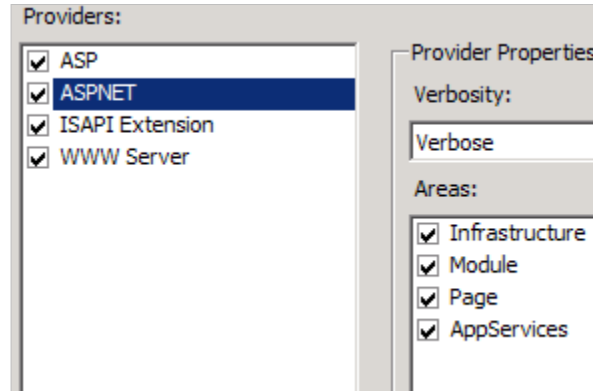


Figure 64 - Selecting Trace Providers

- ▶ **ASP** – allows you to trace the start and completion of an ASP request.
- ▶ **ASPNET** – allows you to trace ASPX requests. Note that if you select this setting, under **Areas** select one or more of the following:
 - **Infrastructure** – trace events that are related to the ASP.NET infrastructure.
 - **Module** – trace events as a request enters and leaves http pipeline modules.
 - **Page** – trace events that are related to the execution of specific ASP.NET page-related events.
 - **AppServices** – trace events that are part of the application services.
- ▶ **ISAPI Extension** – allows tracing requests in and out of an ISAPI extension process.
- ▶ **WWW Server** – allows you to trace requests through the IIS worker process. Note that if you select this setting, under **Areas** select one or more of the following:
 - **Authentication** – trace authentication attempts.
 - **Security** – trace requests that are rejected by the IIS server for security reasons.
 - **Filter** – specify how long ISAPI filter to process requests should take.
 - **StaticFile** – trace the time it takes requests for static files to complete.
 - **CGI** – trace requests for a CGI file.
 - **Compression** – trace compressed responses.
 - **Cache** – trace for cache operations associated with the request.
 - **RequestNotifications** – capture all request notifications.
 - **Module** – trace requests that enters and leaves http pipeline modules, or trace managed modules.

7. In the **Select Trace Providers** dialog box, under **Verbosity** select one or more of the following verbosity levels:
 - ▶ **General**
 - ▶ **Critical Errors**
 - ▶ **Errors**
 - ▶ **Warnings**
 - ▶ **Information**
 - ▶ **Verbose**
8. Click **Finish**.

Using Command Line Tool APPCMD

The APPCMD command-line tool eliminates the need to know an object-oriented programming language. Most of the properties and methods exposed by the IIS objects are accessible through the APPCMD command. The syntax for the APPCMD command is listed below:

```
APPCMD (command) (object-type) <identifier> < /parameter1:value1 ...
```

The **command** is the action performed on the object-type. Below are the list available commands:

- **LIST** – used to list objects and find objects based on matching rules.
- **ADD** – used to create objects.
- **DELETE** – used to delete objects.
- **SET** – used to set parameters on objects.

Note that you can also use START and STOP commands. For example, these commands can be used to start and stop sites and application pools.

The available object-types are listed in the below table:

Object Type	Description
APP	Administration of applications
APPPPOOL	Administration of application pools
BACKUP	Management of server configuration backups
CONFIG	Administration of general configuration sections
MODULE	Administration of server modules
REQUEST	Display of active HTTP requests
WP	Administration of worker processes
SITE	Administration of virtual sites
TRACE	Management of server trace logs
VDIR	Administration of virtual directories

Table 2 - APPCMD Object Types

IIS 7.5

Windows Server 2008 R2 and Windows 7 implement a new version of the IIS server role known as IIS 7.5. The following enhancements have been made to the IIS 7.5 server role:

- **IIS Best Practices Analyzer (BPA)**
The IIS BPA is accessed in Server Manager like the other BPAs introduced in Windows Server 2008 R2. It scans your IIS implementation looking for potential configuration settings that could result in stability or security problems.
- **Windows PowerShell snap-in**
The Web Server or IIS Administration cmdlets are available as part of the WebAdministration module. The module is added to a PowerShell session with the add-psnapin WebAdministration command. Once installed, it provides more than fifty cmdlets.
- **Managed service accounts**
Borrowing from SharePoint 2010 and other newer Microsoft add-on server applications, IIS 7.5 now has the internal ability to use managed services accounts for application pools. This means that the application pool account password can be managed automatically by IIS and be changed within the parameters of the network's password policies.
- **Extension modules now incorporated**
Several modules were available for IIS 7.0 as extension modules and are now incorporated into IIS 7.5 or have been further enhanced in this version. The WebDAV and FTP functionality has been enhanced with new features for reliable and secure content publishing. Request Filtering is now incorporated and helps to prevent harmful request from reaching the server by allowing administrators to block specified HTTP request types. The Configure Editor and User Interface extensions are not incorporated into the IIS Manager.

Manage Web Sites

Managing web sites can be accomplished by using IIS manager. You can think of a web site as a container and within the container, you store web applications. A web site listens for requests on ports via the http or https protocol for web applications. You can configure the following settings for web sites:

- **Site name** – unique for each web server.
- **Application pool** – stores web applications in its own worker process or memory location.
- **Physical path** – the physical path of the site content.
- **Site Binding** – determines how the web site listen for requests and consists of the following:
 - ▶ IP address
 - ▶ Port
 - ▶ Host name
- **SSL certificate** – secures communications between the web site and the client.

Create and Publish an IIS Web Site

To create and publish an IIS web site, perform the following:

Navigate to **Start > Administrative Tools > Internet Information Services (IIS) Manager**.

1. In the left pane, click the **Sites** node and click **Add Web Site** in the **Actions** pane.

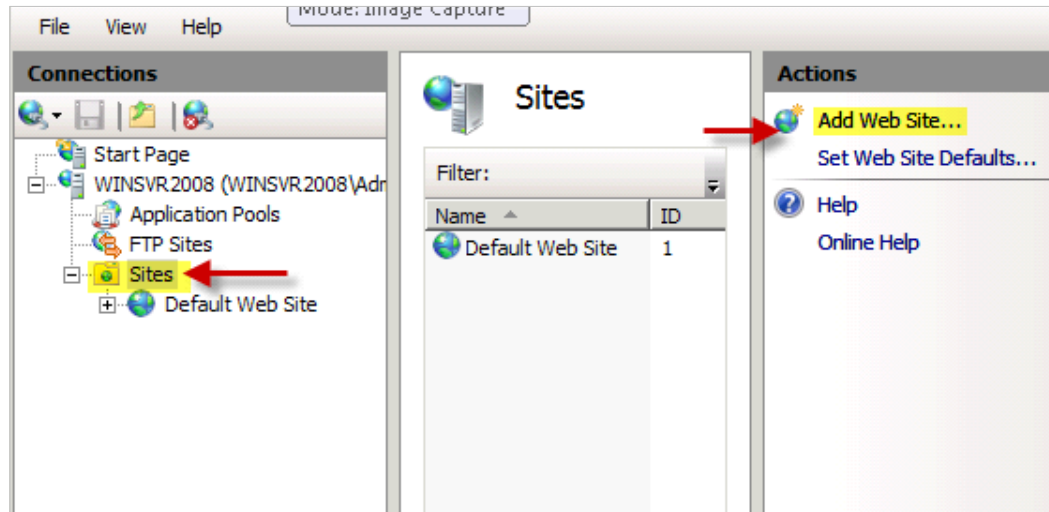


Figure 65 - Adding a Web Site

2. In the **Add Web Site** dialog box, enter a site name in the **Site name** text box.
3. In the **Add Web Site** dialog box, enter the site directory path in the **Physical path** text box.
4. Select from http or https from the **Type** drop-down list.
5. Select an **IP address** or **All Unassigned** to use for the site. Note that your web site can be accessed on all configured IP addresses if you select All Unassigned.
6. To publish the site, enter the **TCP port** number.
7. Enter the **Host Header** name. This actual name that is used to access this site.
8. Ensure **Start Web Site Immediately** is checked.

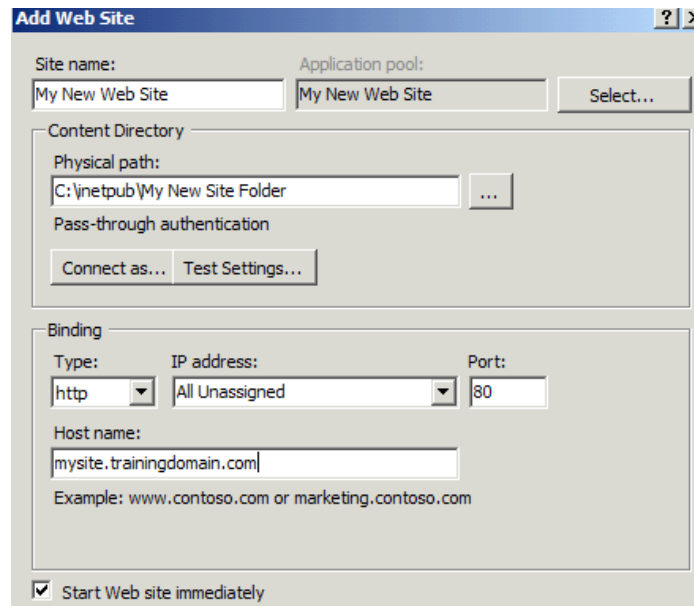


Figure 66 - The Add Web Site Dialogue Box

9. Click **OK**.
10. From Internet Explorer, enter the host header name in the address field.

Configure Virtual Directories

Virtual directories enable the ability to access content located on another computer or a different directory other than your site or application directory.

To create a virtual directory, perform the following:

Navigate to **Start > Administrative Tools > Internet Information Services (IIS) Manager**.

1. In the left pane, right-click the appropriate folder or site.
2. Click **Add Virtual Directory**.

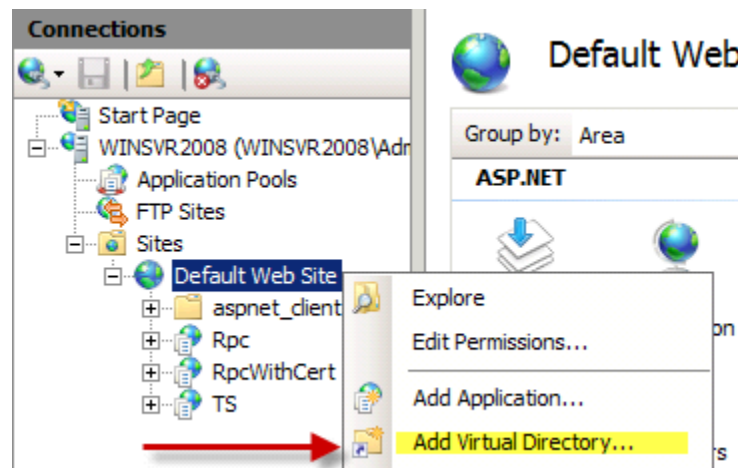


Figure 67 - Adding a Virtual Directory

3. In the **Add Virtual Directory** dialog box, enter a name for your directory in the **Alias** box and browse to the directory location in the **Physical path** box.
4. Note that you can click the **Connect as** button if you don't want to pass user credentials and specify a username and password.

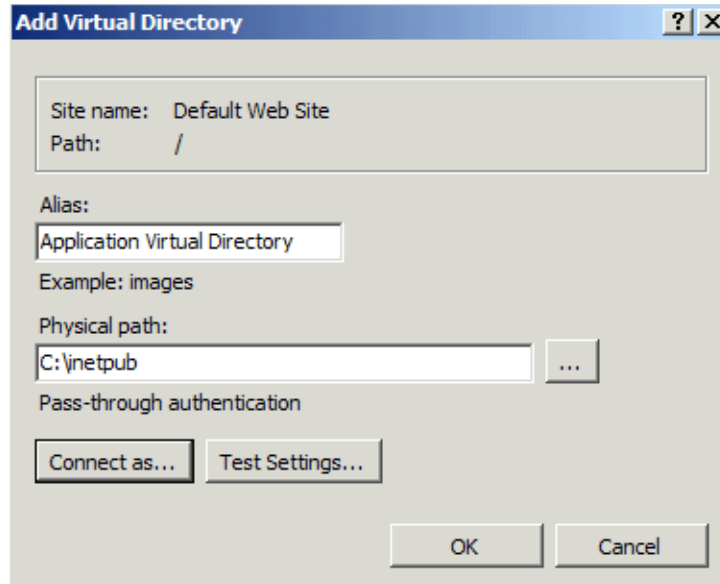


Figure 68 - The Add Virtual Directory Dialogue Box

5. Click **OK**.

Configure Web Site Authentication and Permissions

Web Site Authentication

Authentication is a method by which IIS validates the identity of users accessing content on the web server. The Authentication feature consists of the following modules:

- AD Client Certificate Authentication
- Anonymous Authentication
- ASP.NET Impersonation
- Basic Authentication
- Digest Authentication
- Forms Authentication
- Windows Authentication

Web Site Authorization

After validating a user's identity, the authorization process must go through set of rules and conditions that verify that the identified users can access the intended content. IIS 7.0 provides the following three authorization modules:

- **URL Authorization** – restricts access to content on a web site that should only be access by member of a specified group. You can deny access to sites, applications, directories, or files.
- **Request Filtering** – prevents IIS 7 from processing http requests.
- **IP Authorization** – filters access based on IP address and domain names.

Configuring Web Applications

A Web application is basically a software program that is stored in a web site. It allows users to create, manipulate, and permanently store data. Windows SharePoint Services (WSS) is an example of a web application. WSS is an application that provides a workspace for users to collaborate and store information in a SQL database.

Create a Web Application

To create a web application, perform the following:

Navigate to **Start > Administrative Tools > Internet Information Services (IIS) Manager**.

1. In the left pane, expand the **Sites** node and right-click the web site to store your web application.
2. Click **Add Application**.

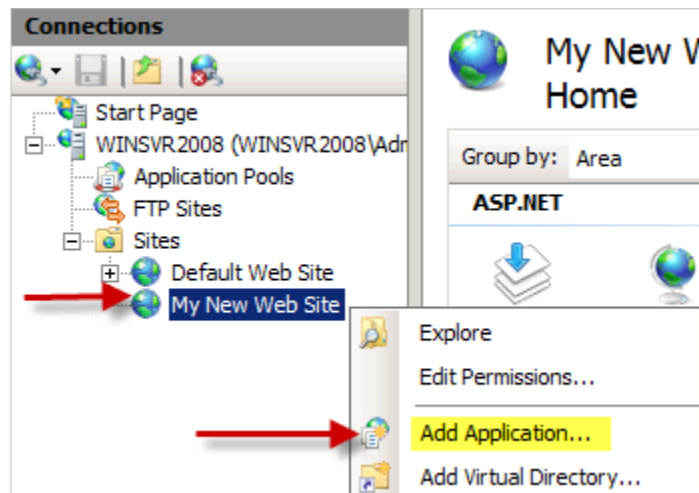


Figure 69 - Creating a Web Application

- In the **Add Application** dialog box, enter a name for your web application URL in the **Alias** box.

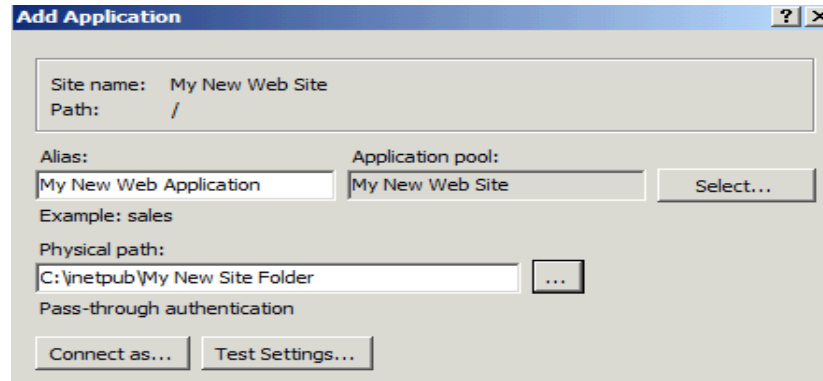


Figure 70 - The Add Application Dialog Box

- If you want to utilize a different application pool, click **Select**.
- Enter a name for your application directory in the **Alias** box and browse to the directory location in the **Physical path** box.
- Note that you can click the **Connect as** button if you don't want to pass user credentials and specify a username and password.
- Click **OK**.

You can also create a web application from the command line using APPCMD. To create an application, use the following syntax:

```
appcmd add app /site.name: string /path: string /physicalPath: string
```

Configure SSL Security

Secure Socket Layer (SSL) is a protocol that provides secure and encrypted communications over the Internet. IIS 7.0 allows you to secure your sites with SSL certificates. Without it you will be transmitting data across the wire in the clear.

Request a Certificate for a Web Site

To request a certificate, perform the following:

Navigate to **Start > Administrative Tools > Internet Information Services (IIS) Manager**.

- In the left pane, click the IIS server name.
- In the middle pane, double click **Server Certificates**.
- In the right pane, click **Request a Certificate**.
- On the **Distinguished Name Properties** page, enter the required information. The **Common name** field is the most important of them all. Clients will use this name to access the web site.
- Click **Next**.
- On the **Online Certification Authority** page, specify an online Certificate Authority and a Friendly name.
- Click **Finish**.

Install a Requested Certificate

To install a requested certificate, perform the following:

Navigate to **Start > Administrative Tools > Internet Information Services (IIS) Manager**.

1. In the left pane, click the IIS server name.
2. In the middle pane, double click **Server Certificates**.

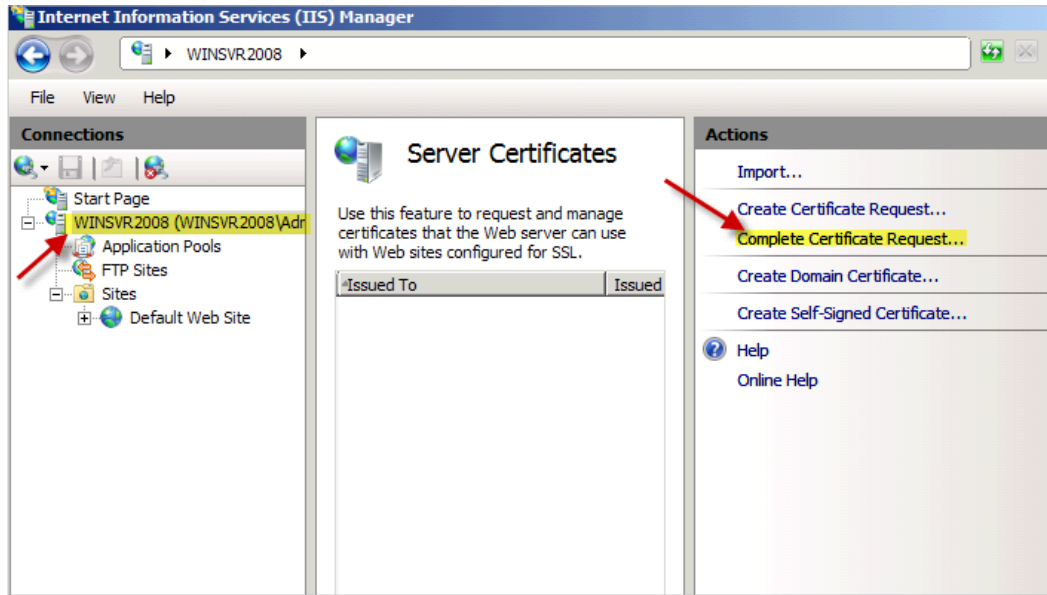


Figure 71 - Installing a Requested Certificate

3. In the right pane, click **Complete Certificate Request**.
4. On the **Specify Certificate Authority Response** page, browse to the **File name containing the certificate authority's response** and enter a friendly name for your certificate.



Figure 72 - Specifying the Certificate Authority Response

5. Click **OK**.

Assign a Certificate to a Website

Once the certificate has been installed, you will need to assign the certificate to a web site.

To assign a certificate to a web site, perform the following:

Navigate to **Start > Administrative Tools > Internet Information Services (IIS) Manager**.

1. In the left pane under **Sites**, click the site you want to SSL enable.

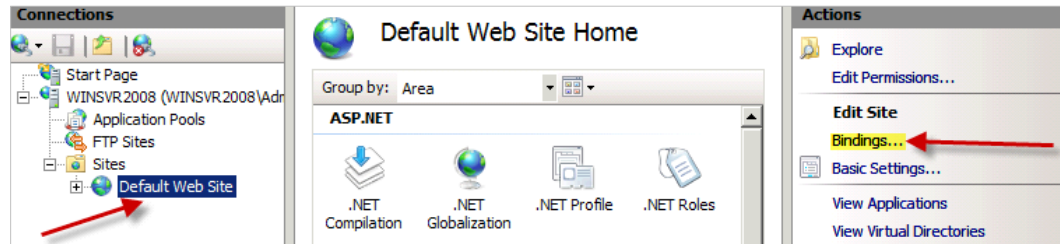


Figure 73 - Assigning a Certificate to a Website

2. In the **Actions** pane, click **Bindings**.
3. In the **Site Bindings** dialog box, click **Add**.

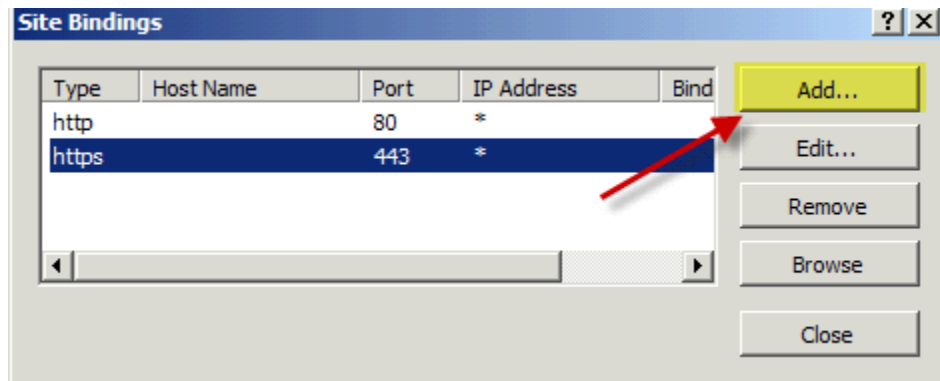


Figure 74 - Creating a Site Binding

4. In the **Add Site Binding** dialog box, select **https** from the **Type** drop-down menu and select the appropriated certificate from the **SSL certificate** drop-down menu.



Figure 75 - Setting Up the Site Binding

5. Click **OK** and then click **Close**.

Configure a File Transfer Protocol (FTP) Server

Configuring File Transfer Protocol (FTP) on a web server will allow users to upload and download files to and from a site. Users will establish connections to your FTP service to access files stored in a designated directory. You first have to install the FTP service and then start the FTP service in order to make it available to users.

Installing FTP

To install the FTP service on Windows Server 2008, perform the following steps:
Navigate to **Start > Administrative Tools > Server Manager**.

1. In the **Server Manager Pane**, under the **Roles Summary** section, click **Web Server (IIS)**.
2. In the **Role Services** section, click **Add Role Services**.
3. Under **Role services**, select **FTP Publishing Service** and click **Next**.
4. Click **Install**.

Starting the FTP Service

To start the FTP service on Windows Server, perform the following steps:
Navigate to **Start > Administrative Tools > Server Manager**.

1. In the **Server Manager** pane, under the **Roles Summary** section, click **Web Server (IIS)**.
2. In the **Web Server (IIS)** section, under **System Services**, click **FTP Publishing Service**.
3. Click **Start**.

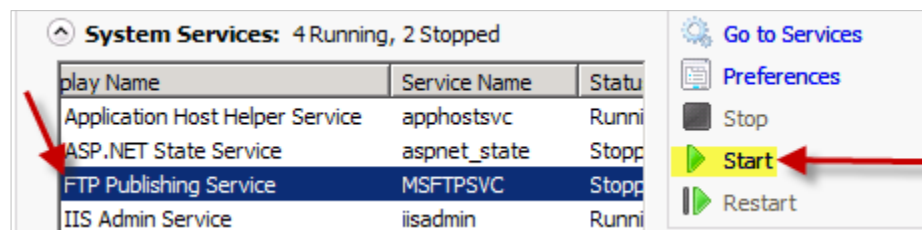


Figure 76 - Starting the FTP Service

Creating a New FTP Site for Authenticated Users

After installing and starting the service, you can enable users to upload and download files from an FTP client. This can be accomplished by creating a new FTP site and configuring FTP authentication.

To create an FTP site, perform the following steps:

Navigate to **Start > Administrative Tools > Internet Information Services (IIS) Manager**.

1. In the **Connections** pane, right-click the **Sites** node and click **Add FTP Site**.
2. On the **Site Information** page, enter an **FTP site name** and browse to the **Physical path** where you want your FTP content to reside.
3. Click **Next**.
4. On the **Site Information** page, select an **IP Address** for the FTP service from the drop-down list and optionally an **SSL** certificate.

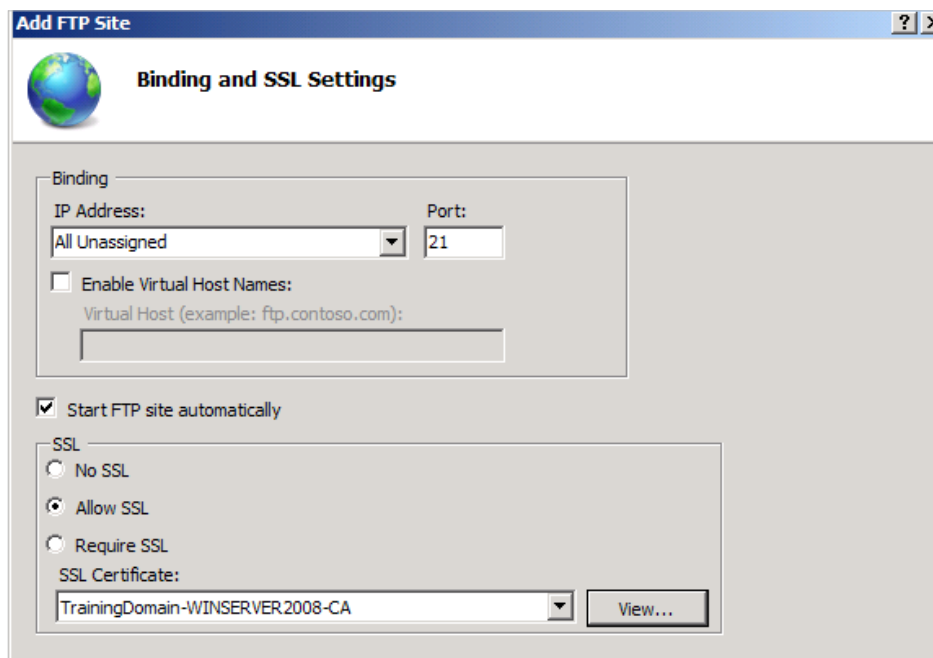


Figure 77 - Binding and SSL Settings

5. Click **Next**.
6. On the **Authentication and Authorization Information** page, you have two choices under the authentication section.

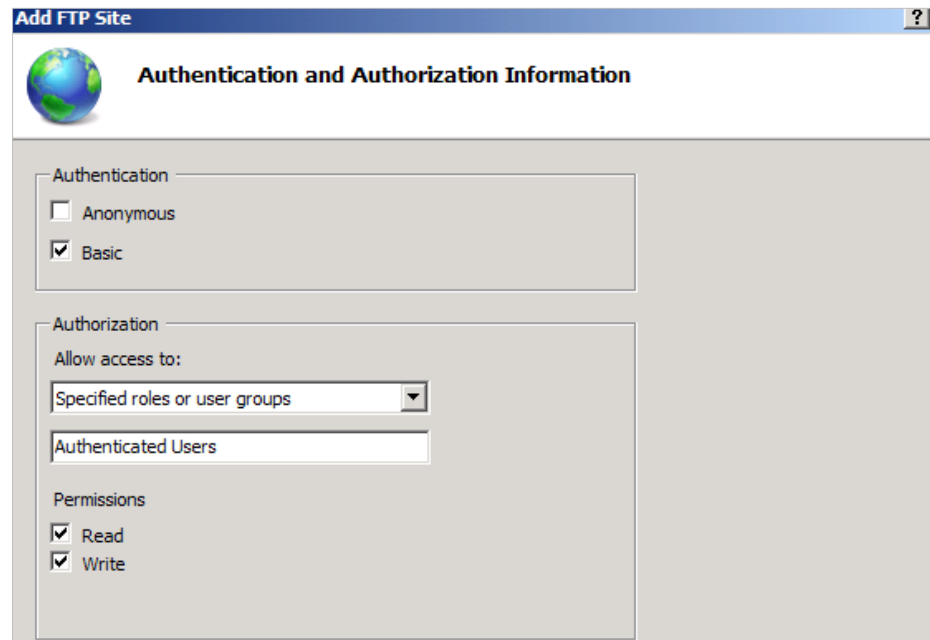


Figure 78 - Authentication and Authorization Information

- ▶ **Anonymous** – any user can access content on the FTP site without a username and password.
 - ▶ **Basic** – forces users to provide a username and password. Note that the username and password are passed in the clear. You should use SSL to encrypt the communication between the client and FTP server.
7. Select **Basic**.
 8. Under the Authorization section, you can **Allow access to** the following:
 - ▶ All Users
 - ▶ All Anonymous Users
 - ▶ Specified roles or user groups
 - ▶ Specified users
 9. Select **Specified roles or user groups** and check **read** and **write** permissions.
 10. Click **Finish**.

Note that you can also create an FTP site by modifying the XML-base applicationHost.config file, which is located in the %systemroot%\System32\inetsrv\config folder.

Configure Simple Mail Transfer Protocol (SMTP)

IIS 7.0 offers the capability to deliver e-mail from your site. You can send mail to a folder for later delivery or immediately to its destination. To configure SMTP e-mail in IIS 7.0, perform the following:

Navigate to **Start > Administrative Tools > Internet Information Services (IIS) Manager**.

1. Select the site-node level for which you want to enable SMTP e-mail. In this case, **Default Web Site** will be selected.

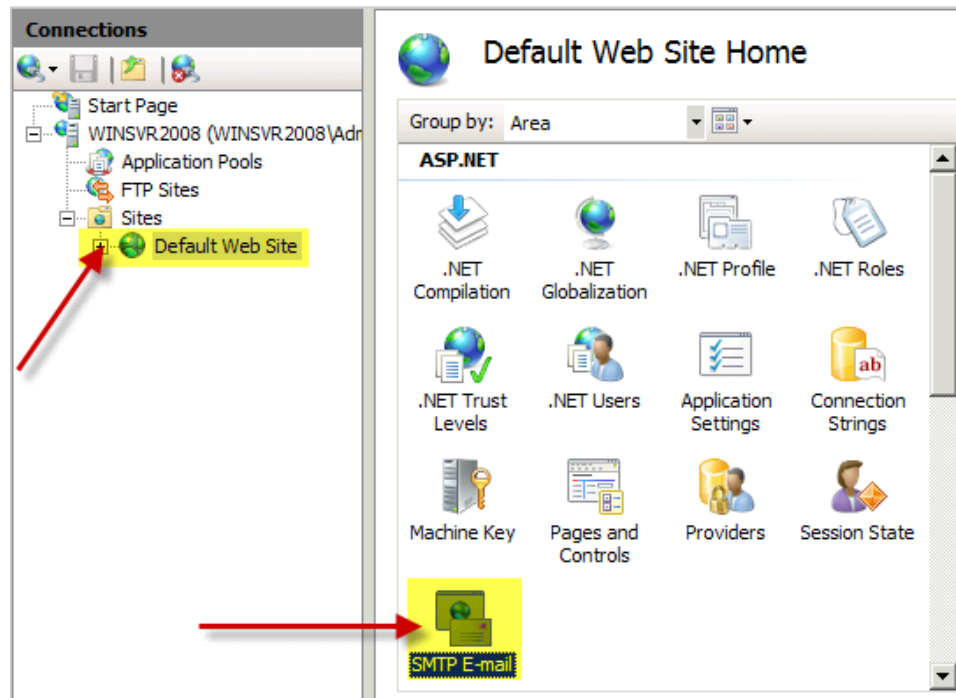


Figure 79 - Configuring SMTP

2. In the **Features View**, double click **SMTP E-mail**.
3. On the **SMTP E-mail** page, enter the e-mail address of the sender.
4. On the **SMTP E-mail** page, you have two options:

Deliver e-mail to SMTP server: ←

SMTP Server:

Use localhost

Port:

Authentication Settings

Not required

Windows

Specify credentials:

Store e-mail in pickup directory: ←

Figure 80 - SMTP Options

- ▶ **Deliver e-mail to SMTP server** – delivers e-mails immediately to an SMTP server.
 - ▶ **Store e-mail in pickup directory** – stores e-mails in a file location allowing ASP.NET applications or users to pickup and deliver messages at a later time.
5. Select **Deliver e-mail to SMTP server** and enter the name of your SMTP server in the SMTP Server text box.
 6. Keep the default TCP port number (25) in the **Port** text box.
 7. Under **Authentication Settings**, you can select “no authentication required; Windows (currently logged user credentials; or specify credentials that the SMTP server will use.
 8. In the **Action** pane, click **Apply**.

Domain 4: Configuring Network Application Services

Configure Windows Media Server

A Windows Media server is intended for streaming on-demand and live media to web browsers and clients running Windows Media Player. It is able to support low-bandwidth and high-bandwidth networks. For example, some company networks experience high network usage during peak hours. Windows Media Server is very resilient in the fact that it can support highly congested networks. It can be configured to offer clients the option of streaming media or downloading media.

- **Streaming** – Windows Media server offers streaming media to clients via the Real Time Streaming Protocol (RTSP). Media is transported using UDP.
- **Downloading** – media from the web using http is downloaded to the client and then processed in Windows Media player. This is not as efficient as streaming from Windows Media server.

Windows Media server supports delivery of the following media formats:

- **Windows Media Video (WMV).**
- **Windows Media Audio (WMA).**
- **MP3.**
- **JPEG** – JPEG supports graphics for playlists.

There are three factors you need to consider before deploying Windows Media server:

- **Bandwidth** – know your network capabilities. Network capacity planning is an essential prerequisite to deploying Windows Media server. Allowing high-quality media streaming during peak hours to five thousand clients is not good planning.
- **Audience** – knowing your audience includes knowing the pattern and behavior of the users on the network. How many users are using dial-up? What department uses the most bandwidth during business hours?
- **Content** – determine your bit-rate encoding method during content consideration. Pre-recorded and live media goes through the encoding process.

To configure Windows Media server, perform the following:

1. Download and run the MSU file (KB934518) for the Streaming Media Service role.
2. Once installed, navigate to **Start > Administrative Tools > Server Manager**.
3. In the **Server Manager** pane, under the **Roles Summary** section, click **Add Roles**.
4. On the **Before You Begin** page, click **Next**.
5. On the **Select Server Roles** page, select **Streaming Media Service** and click **Next**.

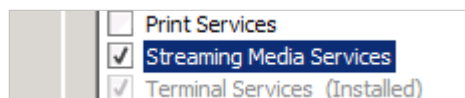


Figure 81 - Adding the Streaming Media Service

6. Click **Next**.

7. On the **Select Role Services** page, select the following role services and then click **Next**:
 - ▶ Windows Media Server
 - ▶ Web-Based Administration
 - ▶ Logging Agent
8. On the **Add role services required for Web-based Administration** page, click **Add Required Role Services**, and then click **Next**.
9. On the **Select Data Transfer Protocols** page, you have two options.
 - ▶ Real Time Streaming Protocol (RTSP)
 - ▶ Hypertext Transfer Protocol (HTTP)
10. Select **Real Time Streaming Protocol (RTSP)**, and then click **Next**.
11. On the **Web Server (IIS)** page, click **Next**.
12. On the **Select Role Services** page, click **Next**.
13. On the **Confirm Installation Selections** page, click **Install**.
14. On the **Installation Results** page, review your results and click **Close**.

Creating a Publishing Point

There are two ways of streaming prerecorded and live content:

- **On-Demand Publishing Point** – offers users the ability to start, stop, pause, fast-forward, and rewind content.
- **Broadcast Publishing Point** – works well for live meetings and company presentations. This works as if it were broadcast as a television program.

To configure a Publishing Point, perform the following:

Navigate to **Start > Administrative Tools > Windows Media Services**.

1. Expand your Windows Media Service server name.

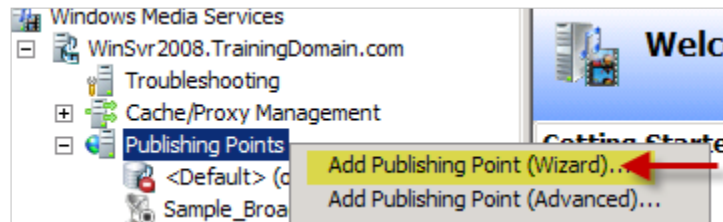


Figure 82 - Adding a Publishing Point

2. Right-click the **Publishing Points** node and then click **Add Publishing Point (Wizard)**.
3. On the **Welcome to the Add Publishing Point Wizard** page, click **Next**.
4. On the **Publishing Point Name** page, entering a meaningful name for your publishing point in the **Name** field and click **Next**.

5. On the Content Type page, you have four options:
 - ▶ **Encoder** – enables live streaming.
 - ▶ **Playlist** – enables a mix file and live streams that you can combine into a continuous stream.
 - ▶ **One file** – useful for the broadcasting of an archived file.
 - ▶ **Files** – enables on-demand playback through a single publishing point.
6. Select **One file** and click **Next**.
7. On the **Publishing Point Type** page, you have two choices:
 - ▶ **Broadcast publishing point** – broadcasts media files (just as a broadcasted television show) that clients can view at the same time.
 - ▶ **On-demand publishing point** – enables clients to control the stream. For example, clients are able to fast-forward, rewind, and pause.
8. Select **On-demand publishing point**, and then click **Next**.
9. On the **Existing Publish Point** page, select **Add a new publishing point** and click **Next**.

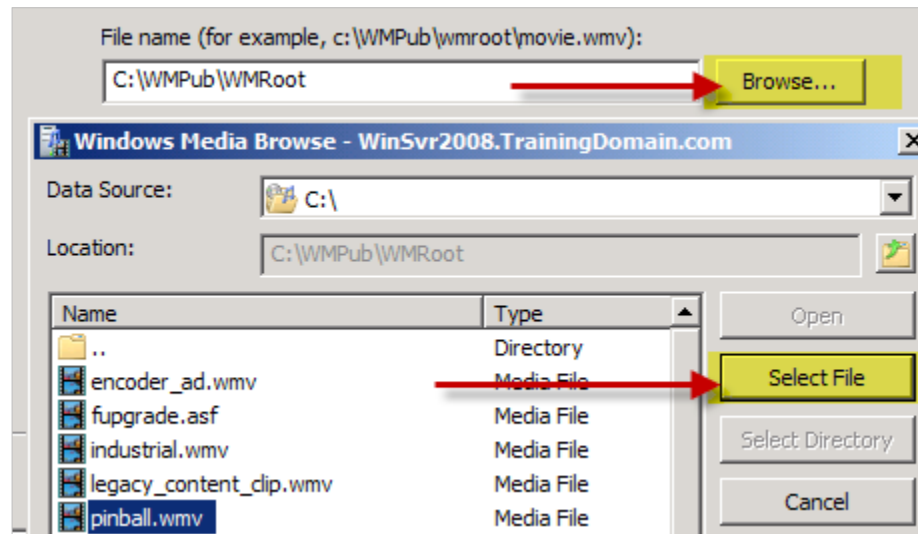


Figure 83 - Adding Files to the Publishing Point

10. On the **File Location** page, click **Browse**.
11. In the **Windows Media Browse** dialog box, choose your file, and then click **Select File**.
12. Click **Next**.
13. On the **Unicast Logging** page, select **Yes, enable logging for this publishing point** and click **Next**.
14. On the **Publishing Point Summary** page, review the summary and click **Next**.
15. On the Completing the Add Publishing Point Wizard page, you have three choices:
 - ▶ Create an announcement file (.asx) or web page (.htm).
 - ▶ Create a wrapper playlist (.wsx).
 - ▶ Create a wrapper playlist (.wsx) and announcement file (.asx) or Web page (.htm).

16. Check **After the wizard finishes** and select **Create an announcement file (.asx) or Web page (.htm)**, and then click **Finish**.
17. On the **Welcome to the Unicast Announcement Wizard** page, click **Next**.
18. On the **Access the Content** page, enter the location where you video and audio will reside and click **Next**.
19. On the **Save Announcement Options** page, enter a location for the announcement file and check **Create a Web page with an embedded player and a link to the content**.
20. Click **Next**.
21. On the **Edit Announcement Metadata** page, enter information about the announcement. This information is displayed during playback of your content. You can enter the following information:
 - ▶ **Title**
 - ▶ **Author**
 - ▶ **Copyright**
 - ▶ **Banner**
 - ▶ **LogURL**
22. Click **Next**.
23. On the **Completing Unicast Announcement Wizard** page, click **Finish**.

Caching and Proxy

Within Windows Server 2008, you can configure Windows Media server as a Cache/Proxy server or a reverse proxy server. A reverse proxy server can provide caching and proxying to other Windows Media servers. Enabling the ability to cache and proxy within a Windows Media server saves bandwidth and balances the load of multiple media servers. You have the choice of caching streaming on-demand content or proxying a live stream. This feature is a built-in Cache/Proxy plug-in available in Windows Server 2008.

Configure Digital Rights Management (DRM)

Windows Server 2008 Digital Rights Manager protects and secures the delivery of digital media files for playback on clients. Below are the phases of the Windows Rights Manager process:

- **Protecting** – business and distribution rules are added to the content. For example, you can set the license validity duration and counted operations (number of playback times).
- **Packaging** – the media file is packaged, encrypted, and locked with a key using Windows Media Right Manager.
- **Distribution** – the package can be downloaded from a web site, streamed from a media server, or placed on a CD.
- **Establishing a License Server** – the provider chooses a clearing house that will store the rights and rules of the license. Clients will validate content via this clearing house.
- **License Acquisition** – during this phase, the client must request a license key before playing the media file.
- **Playing the File** – during this phase, as long as the client media player supports Windows Media Right Manger, users can play the media file according to the specified rules.

Configuring Windows SharePoint Services

As discussed previously, a web site is a container for web applications. Windows SharePoint Services (WSS), a free add-on to Windows Server 2008, is a web application built on ASP.NET 2.0. WSS provides a workspace for users to collaborate and store information in a SQL database. WSS offers users a unique experience through the following:

- **Master Page Integration** – offers users the same look and feel throughout WSS web sites. The master page is used to define the header, footer, and navigation tools. The page layout works in conjunction with the master page. A page layout is a template for content pages.
- **Content Types** – metadata that defines content (fields and columns) for documents, lists, and libraries.
- **Versioning** – allows users to revert back to previous documents.
- **Workflows** – the programmatic representation of an organizations business process. For example, this includes approval processes and document dispositions.

A SharePoint site collection is a hierarchical site structure that contains a top-level site and one or more subsites. Sites within a site collection share common themes such as content types and a web page look and feel.

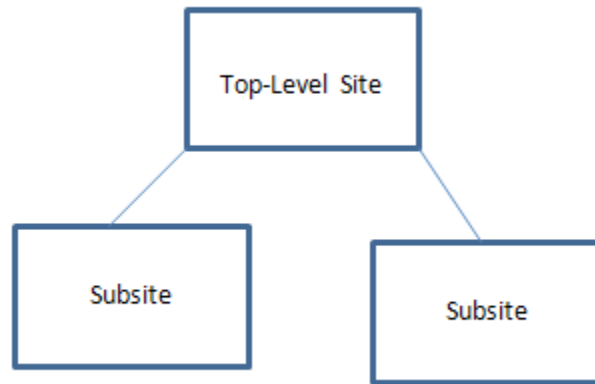


Figure 84 - A SharePoint Site Structure

WSS contains many features. A feature is a set of files and configuration settings made available to every site in a site collection. A WSS farm contains some of the following features:

- Central Web Administration
- Sites and Work Spaces
- Document Libraries
- Calendars
- Task Lists

Installing Windows SharePoint Services Stand-Alone

To install a WSS stand-alone, perform the following: At minimum, you must download and run the SharePoint 3.0 service pack 1 executable for Windows Server 2008.

1. On the **Read the Microsoft Software License Terms** page, check **Accept the terms of this agreement** and then click **Continue**.
2. On the **Choose the installation you want** page, you have two choices:
 - ▶ **Basic** – installs a single standalone server.
 - ▶ **Advanced** – installs a single server or a SharePoint farm.
3. For a stand-alone installation, select **Basic**. The installation process will now begin.
4. The SharePoint setup process will now present you with the SharePoint Products and Technologies Configuration Wizard in order to finalize the installation.
5. On the **Welcome** page click **Next**, and then restart your computer.

Installing Windows SharePoint Services Farm

To install a WSS Farm, perform the following: At minimum, you must download and run the SharePoint 3.0 service pack 1 executable for Windows Server 2008.

1. On the **Read the Microsoft Software License Terms** page, check **Accept the terms of this agreement** and then click **Continue**.
2. On the **Choose the installation you want** page, you have two choices:
 - ▶ **Basic** - This setting installs a single standalone server.
 - ▶ **Advanced** - This setting installs a single server or a SharePoint farm.
3. Select **Advanced**.
4. On the **Server Type** page, select **Web Front End** and click **Install Now**. This will start the installation process.
5. Once the installation process is complete, click **Close**.
6. On the **Welcome** page, click **Next**.
7. Click **Yes** if you are prompted to start the following services:
 - ▶ Internet Information Services.
 - ▶ SharePoint Administration Service.
 - ▶ SharePoint Timer Service.
8. On the Specify Configuration Database settings page, specify the following:
 - ▶ **Database Server**.
 - ▶ **Access Account Username**.
 - ▶ **Password** used to access the database.

9. On the **Configure SharePoint Central Administration Web Application** page, you can override the following:
 - ▶ Port number for the Central Administration site.
 - ▶ Authentication method:
 - **NTLM** - This authentication method is a “challenge and response” protocol introduced in older versions of Windows.
 - **Kerberos** - This authentication method is a “Ticket-Granting-Ticket” system that supports smartcard logon.
10. On the **Completing the SharePoint Products and Technologies Configuration Wizard** page, click **Next**.
11. Click **Finish**.

Using STSadm

STSadm is a command-line tool that offers the ability to administer WSS through a series of commands. You can manage practically all aspects of WSS using STSadmin. Using STSadm, you can manage sites, site collections, backups of site collections, permissions, and others.

For a site collection backup, run the following command:

```
stsadm -o backup -url <URL name> -filename <file name>
```

For a site collection restore, run the following command:

```
stsadm -o restore -url <URL name> -filename <file name> [-hostheaderwebapplicationurl] <Web application URL> [-overwrite]
```

Antivirus

To configure WSS e-mail integration, perform the following steps:

Navigate to **Start > Administrative Tools > SharePoint 3.0 Central Administration**.

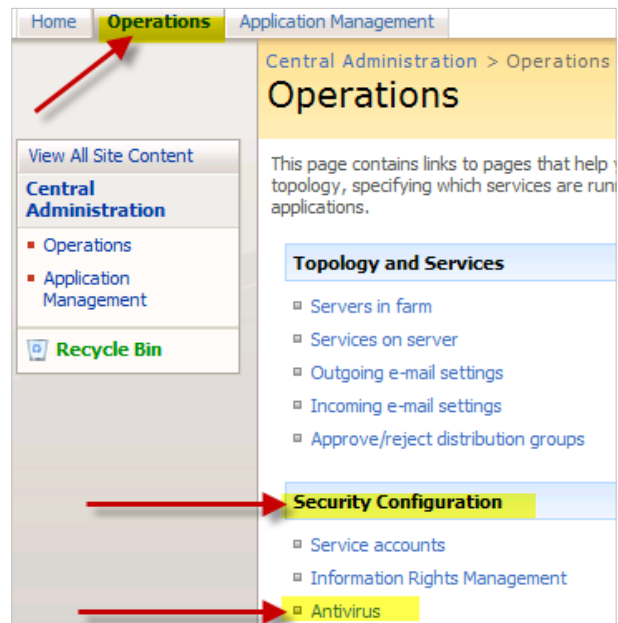


Figure 85 - Installing Antivirus

1. Click the **Operations** tab; under **Security Configuration**, click **Antivirus**.
2. Under the **Antivirus Settings** section, you have four options:

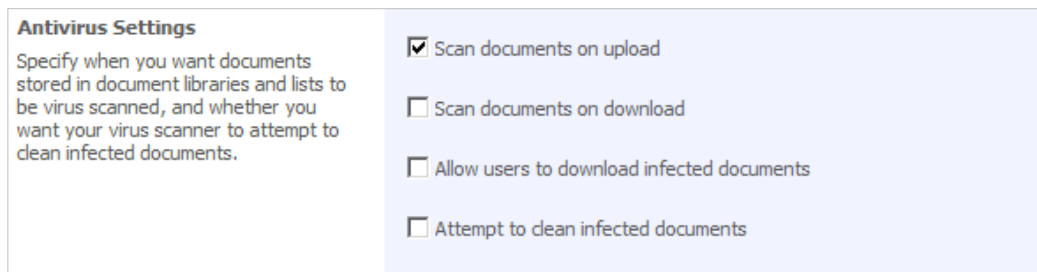


Figure 86 - Antivirus Settings

- ▶ Scan documents on upload
 - ▶ Scan document on download
 - ▶ Allow users to download infected documents
 - ▶ Attempt to clean infected documents
3. Under the **Antivirus Time Out** settings section, enter a time-out duration specifying how long the antivirus scanner should run before timing out.
 4. Under the **Antivirus Threads** settings section, enter the number of execution threads the virus scanner can use.
 5. Click **OK**.

Configuring WSS Services Service Accounts

It is best practice to manage SharePoint with least-privilege administration. This states that administrators should only be given permissions to what they need—nothing more. WSS accounts can be grouped in accordance with its responsibility and scope as follows:

- **Server Farm-Level Accounts** – this account should be used for the following purposes:
 - ▶ SQL Server service account.
 - ▶ WSS Setup account.
 - ▶ Application pool identity account for the Central Administration web site.
- **WSS Search Accounts:**
 - ▶ WSS Search service account.
 - ▶ WSS Search content access account – used to crawl content across sites.
- **Application Pool Identity Accounts** – used to access content databases linked with web applications.

To configure WSS service accounts, perform the following steps:

Navigate to **Start > Administrative Tools > SharePoint 3.0 Central Administration**.

1. Click the **Operations** tab; under **Security Configuration**, click **Service Accounts**.
2. In the **Credential Management** section, configure the service accounts, application pool account, and Central Administration account and then click **OK**.

Figure 87 - Configuring WSS Services Service Accounts

Configure WSS for E-mail Integration

Configuring WSS for e-mail integration involves four steps.

1. Install and Configure the SMTP Service feature.
2. Create an OU in Active Directory and delegate permissions to the application pool account configured earlier in this chapter.
3. Configure incoming e-mail using Central Administration at the server level and on a document library.

To configure SMTP Service, perform the following:

Navigate to **Start > Administrative Tools > Server Manager**.

1. In the left pane, select the **Features** node.
2. In the **Features Summary** pane, click **Add Features**.
3. On the **Select Features** page, select **SMTP Server**.
4. On the **Add features required for SMTP Server** page, click **Add Required Features**.
5. Click **Next**.
6. On the **Confirm Installation Selections** page, click **Install**.
7. Click **Close**.
8. In Windows Explorer, navigate to the SMTP drop folder (c:\inetpub\mailroot\drop).
9. Right the drop folder and select **Properties**.
10. Click the **Security** tab and then click **Edit**.
11. Click **Add** and then add the following local groups:
 - ▶ **WSS_WPG**
 - ▶ **WSS_ADMIN_WPG**
12. Click **OK**.
13. Ensure an MX record is added to the DNS server for your SharePoint site FQDN.

To configure WSS incoming email, perform the following:

Navigate to **Start > Administrative Tools > SharePoint 3.0 Central Administration**.

1. Click the **Operations** tab; under **Topology and Services**, click **Incoming e-mail settings**.

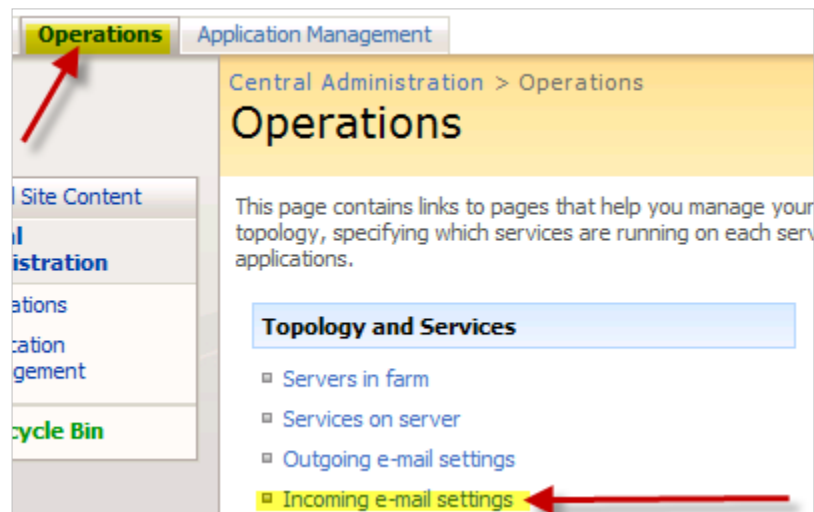


Figure 88 - Configuring the WSS Incoming Email

2. On the **Configure Incoming E-mail Settings** page on the **Enable Incoming Email** section, select **Yes** to enable sites on this server to receive e-mail.

Enable sites on this server to receive e-mail?

Yes No

Settings mode:

Automatic Advanced

Figure 89 - Enabling Incoming Email

3. In the **Directory Management Service** section, select **Yes** to enable the creation of distribution groups and contacts in the OU created earlier in this chapter. You will also need to specify the OU where the distributions groups and contacts will be created.
4. In the **Incoming E-Mail Server Display Address** section, enter the e-mail server address that will be displayed in web pages when users create an incoming e-mail address for a site or list.
5. In the **Safe E-Mail Servers** section, you can restrict to only allow from a list of acceptable e-mail servers.

Safe E-Mail Servers

Specify whether to restrict the set of e-mail servers that can route mail directly to this server farm. This setting can help ensure the authenticity of e-mail stored in SharePoint sites.

Accept mail from all e-mail servers

Accept mail from these safe e-mail servers:

[Empty list box with up and down arrows]

Figure 90 - Configuring Safe Email Servers

To configure WSS site incoming e-mail for a list, perform the following: Using Internet Explorer, open a SharePoint site with a list or library that you want to enable for incoming e-mail.

1. Open the list or library.
2. From the **Settings** menu select **Settings**.
3. On the **Settings** page under the **Communications** sections, click the **Incoming E-mail Settings** link.

Incoming E-Mail Settings: Shared Documents	
Use this page to change the e-mail settings of this document library. You can set the e-mail address for this document library, choose to save or discard e-mail attachments, and set e-mail security policy.	
Incoming E-Mail Specify whether to allow items to be added to this document library through e-mail. Users can send e-mail messages directly to the document library by using the e-mail address you specify.	Allow this document library to receive e-mail? <input type="radio"/> Yes <input checked="" type="radio"/> No E-mail address: <input type="text"/> @WinSvr2008.TrainingDomain.com
E-Mail Attachments Specify whether to group attachments in folders, and whether to overwrite existing files with the same name as incoming files.	Group attachments in folders? <input checked="" type="radio"/> Save all attachments in root folder <input type="radio"/> Save all attachments in folders grouped by e-mail subject <input type="radio"/> Save all attachments in folders grouped by e-mail sender Overwrite files with the same name? <input type="radio"/> Yes <input checked="" type="radio"/> No
E-Mail Message Specify whether to save the original .eml file for an incoming e-mail message.	Save original e-mail? <input type="radio"/> Yes <input checked="" type="radio"/> No
E-Mail Meeting Invitations Specify whether to save e-mailed meeting invitations in this document library.	Save meeting invitations? <input type="radio"/> Yes <input checked="" type="radio"/> No
E-Mail Security Use document library security for e-mail to ensure that only users who can write to the document library can send e-mail to the document library.	E-mail security policy: <input checked="" type="radio"/> Accept e-mail messages based on document library permissions <input type="radio"/> Accept e-mail messages from any sender

Figure 91 - Incoming Email Settings

4. On the **Incoming E-Mail Setting** page, in the **Incoming E-mail** section, click **Yes** and provide an e-mail Address alias for the list or library.
5. In the **E-Mail Attachments** Section, specify a method of how to save attachments.
6. In the **E-Mail Message** section, specify whether to save the original message.
7. In the **E-Mail Meeting Invitations** section, specify whether to save meeting invitations.
8. In the **E-Mail Security** section, specify whether to inherit security from the list or library.
9. Click **OK**.

Practice Questions

Chapter 1 Deploying Servers

- You are planning to use Windows Server 2008 and WDS to deploy Windows Vista and Windows Server 2008 machines. In your lab, you have two servers that you plan to configure as test machines for WDS testing. One of the machines is an Itanium-based machine and the other uses standard Intel Xeon processors. What machine and edition of Windows Server 2008 will you use for your test server? Select the best answer.

 - A. Itanium machine running Windows Server 2008 Standard Edition
 - B. Itanium machine running Windows Server 2008 Web Edition
 - C. Xeon machine running Windows Server 2008 Standard Edition
 - D. Xeon machine running Windows Server 2008 Web Edition
- The director of Information Systems has asked you to provide a list of benefits related to virtualization. Which of the following items would you include on this list? Choose all that apply.

 - A. Reduced hardware costs
 - B. Software testing and development is simpler
 - C. Improved hardware redundancy
 - D. Reduced installation times
- You want to enable Hyper-V on a Server Core installation. Which of the following commands will provide the desired result? Select the correct answer.

 - A. `start /w ocsetup Microsoft-Hyper-V`
 - B. `start /w Hyper-V`
 - C. `start /w ocsetup Hyper-V`
 - D. `Enable Hyper-V`
- What two methods may be used to isolate virtual machines onto separate networks on a single Hyper-V host? Choose two.

 - A. Assign different virtual networks to the appropriate virtual machines
 - B. Assign virtual machines to differing VLANs
 - C. You cannot do this and you must install the virtual machines on separate physical hosts
 - D. Install multiple physical NICs in the Hyper-V host

5. You have created a virtual machine running Windows Server 2008 Web Edition as the guest operating system. The server has 8 GB of RAM and the stated virtual machine is the only function running on the server other than standard operating system tasks. The server has two dual-core processors running at 3 GHz each. The virtual disk is stored on a RAID 0 three drive array and each drive is a SATA 10,000 RPM drive. The virtual machine performs well when users access the web services from remote; however, the performance is very poor when an administrator accesses the virtual machine for administration. Additionally, the mouse acts sporadic and the graphics seem to be very slow. What should you try in order to resolve these problems? Select the best answer.
- A. Reinstall the virtual machine
 - B. Search for update mouse and video drivers for your video card on the Internet
 - C. Install the Hyper-V Integration Services
 - D. Replace the mouse and video card
6. You want to configure a folder on one volume to point to a pointer to the root directory of another volume. What storage mechanism do you need to implement? Select the best answer.
- A. RAID 1
 - B. Sparse file
 - C. Shared drive
 - D. Mount point
7. You want to extend a simple volume to use 100 GB of space on a newly installed physical disk. The existing volume is a partition on a basic disk and it is formatted as NTFS. The volume is used for user data only. You require that the space on the new physical disk be consumed into the existing volume so that users can store data there. You use the Server Manager and the Disk Management node to perform the action. When you right click on the exiting volume to select the Extend Volume option, it is not available. What is the problem? Select the best answer.
- A. The disk must be converted to a dynamic disk first.
 - B. You cannot extend the disk. Delete the volume and create a striped volume and then reformat the new spanned volume.
 - C. You cannot extend a data volume. You can only extend the boot or system volume.
 - D. Only existing spanned volumes can be extended.

Chapter 2

Configuring Terminal Services

1. You are implementing Terminal Services with Windows Server 2008. You want clients to connect to the Terminal Services server using a web browser. You further want the clients to be able to control a complete desktop environment through the browser-based Terminal Services connection. What feature do you need to configure in order to enable this kind of access? Select the best answer.
- A. TS RemoteApp
 - B. TS Remote Desktop Web Connection
 - C. Remote Desktop
 - D. Remote Registry

2. What service, in addition to the Terminal Services role service, is needed in order to enable TS RemoteApp? Select the best answer.
- A. No other service is needed
 - B. Internet Information Services
 - C. Remote Registry
 - D. TS RemoteConnect
3. You have been asked to configure TS Gateway. You have installed an SSL certificate that is self-signed. You have also mapped the SSL certificate to the TS Gateway Server. What three tasks remain? Choose the three correct answers.
- A. Add the TS Gateway Server to an AD domain
 - B. Create a CAP
 - C. Create a RAP
 - D. Open port 1443 on the firewall
4. You are implementing the TS Gateway role and you must ensure that the dependent roles are already installed. What roles are required by TS Gateway? Choose all that apply.
- A. Web Server (IIS 7.0)
 - B. Network Policy and Access Services
 - C. Remote Procedure Call (RPC) over HTTP proxy
 - D. ISA Server
5. You have implemented a terminal server farm consisting of two servers. One server is much more powerful than the other. You want to ensure that the more powerful server receives twice as many connections as the less powerful server. How can you accomplish this? Select the best single answer.
- A. Set the relative weight of the less powerful server to 300
 - B. Set the relative weight of the less powerful server to 100
 - C. Set the relative weight for the more powerful server to 200
 - D. Set the relative weight of the more powerful server to 50
6. You want to ensure that the Terminal Services processes get a higher priority on a particular Windows Server 2008 machine that is also running IIS. Lately, users have complained that their Terminal Services sessions often perform poorly. You've noticed that this usually happens when the IIS service is being used heavily. What feature can you install on the Windows Server in order to gain control over the processor and memory utilization so that you can give a higher priority to the Terminal Services process? Select the best answer.
- A. .Net Framework 3.0
 - B. Windows System Resource Manager
 - C. Failover Clustering
 - D. Simple Network Management Protocol

7. You want to limit the terminal servers allowed to communicate with license servers in a given domain. How would you accomplish this? Select the best answer.
- A. Add only the terminal servers that you want to communicate with the license server to the Terminal Server Computers group in Active Directory
 - B. Configure the allowed servers list on the security tab of the license server dialog
 - C. Set the Group Policy for the Allows Terminal Servers policy in the Default Domain Policy GPO
 - D. Change the Automatically discover a license server setting to Use the specified license servers

Chapter 3

Configuring a Web Services Infrastructure

1. In which file are the configuration settings stored for each website and in what location is the file stored? Select the best answer.
- A. The file is web.config and it is stored in the root of each website
 - B. The file is system.application and it is stored in the root of each website
 - C. The file is applicationhost.config and it is stored in the root of each website
 - D. The file is web.config and it is stored in the %windir%\system32 folder
2. You need to support a web application that is based on the architecture of IIS 6. The application will be running on a Windows 2008 Server that implements IIS 7. What non-default features will need to be installed? Select the best answer.
- A. ApplicationHost.config file
 - B. IIS 6 Upgrade Manager
 - C. Classic pipeline mode
 - D. Backward-compatibility features
3. You have installed the FTP Role Service on the server at 134.12.15.89. When users attempt to connect, they are unable to reach the FTP server. The server is on your private network and your Internet connection passes through a firewall. The users are attempting to connect through the Internet using their home systems. Only standard FTP is being used with no enhanced security. What action should you take? Select the best answer.
- A. Open port 21 in the firewall for 134.12.15.89
 - B. Open port 21 in the firewall for the entire network
 - C. Open port 80 in the firewall for 134.12.15.89
 - D. Open port 80 in the firewall for the entire network
4. You have installed the SMTP service that ships with Windows 2008 Server. What tool will you use to manage the SMTP service? Select the best answer.
- A. SMTP Manager
 - B. Internet Information Services (IIS) Manager
 - C. Internet Information Services (IIS) 6.0 Manager
 - D. SMTP 6.0 Manager

5. You need to configure .NET Framework settings globally. What file will you use? Select the best answer.
- A. ApplicationHost.config
 - B. Redirection.config
 - C. Machine.config
 - D. CLR.config
6. You have installed an IIS 7 web server. You've made no configuration changes. What account will be used for anonymous access? Select the best answer.
- A. IUSR
 - B. Guest
 - C. Anonymous
 - D. Default

Chapter 4

Configuring Network Application Services

1. What Windows 2008 Server feature can be used to implement DRM? Select the best answer.
- A. Windows DRM
 - B. AD Rights Management Services
 - C. Network Access Protection
 - D. Network Access Quarantine Control
2. You have implemented business rules through AD RMS. All users utilize Office 2007. How will the sharing of business rules take place? Select the best answer.
- A. Automatically
 - B. Manually
 - C. Through replication
 - D. Through load balancing
3. You have implemented AD RMS. You want to control who has access to the license files and can therefore play media content. What kind of policy will you need to create? Select the best answer.
- A. Revocation Policy
 - B. Trust Policy
 - C. Extended Policy
 - D. Exclusion Policy
4. You work as the server administrator for Midwest Wholesale Mouse Pads, LLC. You are installing SharePoint Services in a standalone deployment model. Which of the following are dependencies that must be added to the server in order to install SharePoint Services? Choose all that apply. Select the best answers.
- A. .NET Framework 3.0
 - B. Internet Information Services
 - C. Windows Internal Database
 - D. SQL Server 2005 Standard Edition or higher

5. You are investigating backup methods available for your WSS 3.0 web server. Which of the following are tools provided by Microsoft? Choose all that apply.
- A. SQL Server backup
 - B. Volume Shadow Copy-based tools
 - C. Built-in WSS Backup tools
 - D. Backup Exec

Answers & Explanations

Chapter 1

1. Answer: C

Explanation A. Incorrect. WDS is not available for Itanium-based systems.

Explanation B. Incorrect. WDS is not available for Itanium-based systems or with the Web Edition.

Explanation C. Correct. The Standard, Enterprise and Datacenter Editions all come with WDS and Xeon installations support WDS unlike Itanium systems, which do not.

Explanation D. Incorrect. WDS is not supported on the Web Edition of Windows Server 2008.

2. Answers: A, B

Explanation A. Correct. Virtualization can reduce hardware costs since it is often less expensive to purchase a single server, which is as powerful as two or more servers, than it is to purchase multiple servers.

Explanation B. Correct. Virtual test servers are very easy to build and behave just like physical servers from a functional perspective.

Explanation C. Incorrect. Virtualization actually placed more on less hardware and may reduce redundancy without the use of multiple virtual servers and a SAN.

Explanation D. Incorrect. It takes just as long to setup a virtual machine as it does to setup a physical machine - sometimes longer. While you can clone a virtual machine, you can also deploy physical machines with images.

3. Answer: A

Explanation A. Correct. This command will enable the Hyper-V role and require a reboot of the machine. To administer the Hyper-V role installed on the Server Core installation, you will need to connect to the server by using Hyper-V Manager from a different system.

Explanation B. Incorrect. This command will not enable the Hyper-V role on a Server Core installation.

Explanation C. Incorrect. This command will not enable the Hyper-V role. It should read, `start /w ocsetup Microsoft-Hyper-V`.

Explanation D. Incorrect. It would be an advantage if it were this simple, but the proper command is just a bit more complex: `start /w ocsetup Microsoft-Hyper-V`.

4. Answers: A, B

Explanation A. Correct. The normal process would be to create distinct virtual networks and then place the virtual machines in the appropriate network.

Explanation B. Correct. Hyper-V does support the use of VLAN IDs within the virtual networks. This means that one virtual network can support all of the virtual machines and you can use VLAN IDs to separate the machines.

Explanation C. Incorrect. This function may be accomplished with distinct virtual networks or differing VLAN IDs.

Explanation D. Incorrect. While this may be beneficial, it is not required and would not automatically cause the virtual machines to be separated.

5. Answer: C

Explanation A. Incorrect. This action will take too long and will not likely resolve the problem.

Explanation B. Incorrect. The virtual machines all have the same emulated hardware and drivers are provided by Microsoft via the Integration Services.

Explanation C. Correct. These symptoms are very common on a Hyper-V server virtual machine without the Integration Services. If they are already installed, try uninstalling them and then reinstalling.

Explanation D. Incorrect. The problem is most likely a lack of Integration Services or a corrupt installation of the same.

6. Answer: D

Explanation A. Incorrect. RAID 1 provides mirroring at the physical drive level.

Explanation B. Incorrect. A sparse file is a file created on an NTFS volume that is filled with NULL data in order to reserve the space quickly.

Explanation C. Incorrect. A shared drive provides network access to file resources.

Explanation D. Correct. An NTFS mount point allows you to have a volume appear as a folder on another volume.

7. Answer: A

Explanation A. Correct. You can only extend volumes on dynamic disks. First, convert the disk to a dynamic disk and then extend the volume.

Explanation B. Incorrect. You can extend the disk. It must be formatted as NTFS and it cannot be the system or boot volume; however, it must also be a dynamic disk.

Explanation C. Incorrect. In fact, the opposite is true. You cannot extend the boot or system volume. You can only extend data volumes.

Explanation D. Incorrect. Simple volumes can be extended. They must be NTFS. They must not include the boot or system volumes. They must be dynamic disks.

Chapter 2

1. Answer: B

Explanation A. Incorrect. TS RemoteApp allows for the publishing of individual applications instead of entire desktops.

Explanation B. Correct. The TS Remote Desktop Web connection feature of TS Web Access allows remote users to connect to the TS desktop and control the remote system according to their permissions.

Explanation C. Incorrect. Remote Desktop does not provide this functionality within a web browser. It only provide remote desktop control through the RDC application.

Explanation D. Incorrect. The remote registry service provides registry access across the network.

2. Answer: A

Explanation A. Correct. The TS RemoteApp functionality is integrated into the Terminal Service role.

Explanation B. Incorrect. If you want to use the TS Web Access function to deploy a RemoteApp, IIS is needed; however, IIS is not needed for normal TS RemoteApp functionality.

Explanation C. Incorrect. Remote registry is install on all Windows machines, but it is not needed for TS RemoteApp.

Explanation D. Incorrect. No such service exists.

3. Answers: A, B, C

Explanation A. Correct. In order to access domain groups and policies, the server must be a member of the AD domain.

Explanation B. Correct. A connection authorization policy (CAP) is used to define constraints within which clients must reside. The TS CAP is used to define groups that may connect and behaviors such as device redirection.

Explanation C. Correct. A resource authorization policy (RAP) defines the network resources to which remote users may connect. It will define the AD group that may use the resource and the port, which is 3389 for RDP.

Explanation D. Incorrect. TCP port 1443 is used by Microsoft SQL Server and is not related to the configuration of TS Gateway.

4. Answers: A, B, C

Explanation A. Correct. The IIS server is the default HTTP endpoint.

Explanation B. Correct. This service provides the CAP and RAP policy functionality required.

Explanation C. Correct. The RPC over HTTP Proxy role enables the core capabilities needed to encapsulate the terminal services communications.

Explanation D. Incorrect. ISA Server is an optional endpoint solution, but it is not required.

5. Answer: C

Explanation A. Incorrect. This would cause the less powerful server to receive three times the connections of the more powerful server.

Explanation B. Incorrect. The default relative weight is 100 so this action will change nothing.

Explanation C. Correct. The default relative weight is 100. By setting it to 200 and leaving the other server at the default, the more powerful server will receive twice as many connections.

Explanation D. Incorrect. This would cause the less powerful server to receive twice as many connections since it will still be set to the default relative weight of 100.

6. Answer: B

Explanation A. Incorrect. The .Net framework is used for application development or to support applications that depend on it, but it cannot help in prioritizing Terminal Services over IIS.

Explanation B. Correct. WSRM is a feature - not a role - that can be installed on any Windows Server 2008 machine. It allows you to set processor and memory utilization rules and to schedule different rules for different times of the day.

Explanation C. Incorrect. Failover Clustering is a feature that can be installed, but it does not provide prioritization of one process over another.

Explanation D. Incorrect. SNMP is used for remote management and documentation of network devices.

7. Answer: A

Explanation A. Correct. This group is used to control which terminal servers may communicate with the license servers in that domain.

Explanation B. Incorrect. No such tab or list exists.

Explanation C. Incorrect. No such policy exists.

Explanation D. Incorrect. This setting is used to force a terminal server to use a specific license server as opposed to preventing it from using one.

Chapter 3**1. Answer: A**

Explanation A. Correct. The web.config file contains website, application or directory settings and is located in the root folder of each website.

Explanation B. Incorrect. The system.applicaton file contains the global settings.

Explanation C. Incorrect. The ApplicaitonHost.config file stores settings for the updated version of the FTP server. The original version of the FTP server stores information in the IIS 6.0 metabase.bin file.

Explanation D. Incorrect. The file is web.config, but it is stored in the root of each website.

2. Answer: D

Explanation A. Incorrect. The ApplicationHost.config file is installed by default.

Explanation B. Incorrect. No such application exists.

Explanation C. Incorrect. This feature is available by default.

Explanation D. Correct. Features such as the IIS 6 Management Compatibility, IIS 6 Metabase Compatibility, IIS 6 WMI Compatibility, IIS 6 Scripting Tools, and IIS 6 Management Console are not installed by default.

3. Answer: A

Explanation A. Correct. By opening the port used by FTP, you will allow the users access.

Explanation B. Incorrect. Only 134.12.15.89 must be allowed for port 21 connections.

Explanation C. Incorrect. Port 80 is used by HTTP by default. Configuring a Web Services Infrastructure 26.

Explanation D. Incorrect. Port 80 is used by HTTP by default and ports should only be opened for the proper destinations.

4. Answer: C

Explanation A. Incorrect. There is no such tool.

Explanation B. Incorrect. The standard IIS Manager, which is designed for the IIS 7 services, does not support the default SMTP service. You must use the IIS 6.0 Manager.

Explanation C. Correct. The IIS 6.0 Manager is used to manage the default SMTP service and this service depends on IIS 6 Metabase Compatibility and the IIS 6 Management Console.

Explanation D. Incorrect. There is no such tool.

5. Answer: C

Explanation A. Incorrect. The ApplicationHost.config file contains settings for the server and defines sites, application pools and virtual directories.

Explanation B. Incorrect. The Redirection.config file tells the server to look in another location for server configuration information.

Explanation C. Correct. The Machine.config file contains .NET settings that apply to all applications running with the Common Language Runtime (CLR).

Explanation D. Incorrect. No such configuration file exists.

6. Answer: A

Explanation A. Correct. The IUSR account is used for anonymous access.

Explanation B. Incorrect. A guest account is not used by IIS 7 in a default installation.

Explanation C. Incorrect. That would make too much sense. Instead, the IUSR account is used.

Explanation D. Incorrect. There is no account named default in an IIS 7 default installation.

Chapter 4**1. Answer: B**

Explanation A. Incorrect. No such feature exists.

Explanation B. Correct. AD RMS is Microsoft's implementation of DRM.

Explanation C. Incorrect. NAP is used to ensure that clients connecting to a Microsoft network include required security settings and applications.

Explanation D. Incorrect. NAQC was the network access protection mechanism for Windows Server 2003-based networks.

2. Answer: A

Explanation A. Correct. Business rules are shared automatically when an AD RMS compatible application creates the content.

Explanation B. Incorrect. Since the users are using an AD RMS compatible application, the business rules will be shared automatically.

Explanation C. Incorrect. Replication is not used for business rule sharing.

Explanation D. Incorrect. Business rules are not shared via load balancing.

3. Answer: D

Explanation A. Incorrect. The Revocation Policy is used to remove access rights from a user who has previously been given access.

Explanation B. Incorrect. Trust policies are used to trust domains outside of your Active Directory domain.

Explanation C. Incorrect. Extended Policies allow the user to view content using different viewers or force the user to retrieve a new license each time the content is viewed.

Explanation D. Correct. You control who may access the media by creating Exclusion Policies.

4. Answers: A, B, C

Explanation A. Correct. The .NET Framework allows many of the components of WSS to operate.

Explanation B. Correct. IIS is used to serve up the SharePoint portal sites.

Explanation C. Correct. This is based on SQL Server technology, but it is used in place of a SQL Server in a standalone deployment.

Explanation D. Incorrect. A server farm deployment would rely on SQL Server 2005. A standalone deployment uses the Windows Internal Database.

5. Answers: A, B, C

Explanation A. Correct. If you have installed WSS to use SQL Server, you can use the built-in SQL Server backup software to backup the SQL Server database tables that are used by WSS.

Explanation B. Correct. These tools offer the ability to take a snapshot of the database without downtime.

Explanation C. Correct. The built-in tools, while limited, can be used to backup everything or selected sections of the WSS sites.

Explanation D. Incorrect. Backup Exec is a third-party backup software program.