

# Upgrading **MCSE 2003** to **Server 2008**

**(70-649)** Microsoft Certified  
IT Professional (MCITP)

 **Smarter  
Training**

This LearnSmart Exam Manual prepares ambitious IT professionals for the Upgrading MCSE 2003 to Server 2008 exam (70-649). By studying this manual, you will become familiar with a wealth of exam-related content, including:

- Configuring Additional Active Directory Server Roles
- Configuring IP Addressing and Services
- Monitoring and Managing a Network Infrastructure
- Additional topics 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!

# Upgrading your MCSE on Server 2003 to Server 2008 (70-649) LearnSmart Exam Manual

Copyright © 2011 by PrepLogic, LLC.  
Product ID: 012199  
Production Date: September 15, 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](mailto:solutions@learnsmartsystems.com)

## International Contact Information

**International:** +1 (813) 769-0920

**United Kingdom:** (0) 20 8816 8036

## Table of Contents

<i>Abstract</i> .....	6
<i>What to Know</i> .....	6
<i>Study Tips</i> .....	7
<b>Configuring Additional Active Directory Server Roles</b> .....	<b>8</b>
Active Directory Lightweight Directory Services – Background and Configuration .....	8
Directory Rights Management Service (AD RMS) – Background and Configuration .....	11
Read Only Domain Controller (RODC) – Background and Configuration .....	15
Active Directory Federation Services (ADFS) – Background and Configuration .....	17
<i>Offline Domain Join</i> .....	25
Configuring IP Addressing and Services .....	25
Configure IPv4 and IPv6 addressing .....	25
<i>IPv6: Syntax</i> .....	26
<i>IPv6: Address Types</i> .....	27
<i>IPv6: Implementing Compatibility</i> .....	29
<i>IPv6: Tools</i> .....	29
<i>IPv6: Configuration</i> .....	30
Configure routing .....	32
Configure IPsec .....	34
<b>Monitoring and Managing a Network Infrastructure</b> .....	<b>38</b>
Configure Windows Software Update Services (WSUS) server settings.....	38
Capture performance data .....	42
<i>Performance Monitor</i> .....	43
<i>Reliability Monitor</i> .....	45
<i>Data Collector Sets</i> .....	46
Monitor event logs .....	47
<i>Application and Service Logs</i> .....	47
<i>Custom Views</i> .....	47
<i>Event Forwarding and Subscriptions</i> .....	48
<i>DNS Logging</i> .....	52
Gather network data.....	52
Microsoft Baseline Security Analyzer .....	52
<i>Simple Network Management Protocol (SNMP)</i> .....	54
<i>Microsoft Network Monitor</i> .....	55

<b>Deploying Servers</b> .....	<b>57</b>
Deploy images by using Windows Deployment Services .....	57
Configure Microsoft Windows activation .....	60
Configure Windows Server Hyper-V and virtual machines .....	63
<i>Hardware requirements</i> .....	63
<i>Physical to Virtual Migrations</i> .....	64
<i>Virtual Hard Disks</i> .....	64
<i>Installing Hyper-V:</i> .....	65
<i>Virtual Networks</i> .....	67
<i>Backups</i> .....	67
Configure high availability .....	68
<i>Failover Clusters</i> .....	69
<i>Network Load Balancing (NLB)</i> .....	71
Configure storage .....	75
<i>Virtual Disk Service (VDS) APIs</i> .....	76
<i>SANs</i> .....	76
<i>SAN Technologies</i> .....	77
<i>Mount Points</i> .....	78
<i>Windows Automated Installation Kit</i> .....	79
<i>Windows Deployment Services</i> .....	80
<i>PXE provider for Transport Server</i> .....	81
<b>Configuring Terminal Services</b> .....	<b>82</b>
Configure Windows Server 2008 Terminal Services RemoteApp (TS RemoteApp) .....	83
<i>Configuring Terminal Services Web Access</i> .....	86
Configure Terminal Services Gateway .....	87
<i>Install and TS Resource Authorization Policy (RAP) Config</i> .....	88
<i>Policy Configuration and Customization</i> .....	89
<i>Certificate Configuration</i> .....	89
<i>Terminal Services Group Policy</i> .....	90
Configure Terminal Services load balancing .....	91
Configure and monitor Terminal Services resources .....	91
<i>Allocating resources by using Windows Server Resource Manager</i> .....	93
<i>Configuring application logging</i> .....	94
Configure Terminal Services licensing .....	94

Deploying licensing server and Managing CALs .....	94
<i>Connectivity between terminal servers and Terminal Services licensing server</i> .....	96
<i>Recovering TS LicenseServer</i> .....	97
Configure Terminal Services client connections .....	97
Connecting local devices and resources to a session .....	97
<i>MSTSC and the Remote Desktop Client</i> .....	98
<i>Terminal Services Profiles and Home Directories</i> .....	100
<i>Single Sign On</i> .....	100
Configure Terminal Services server options .....	101
<b>Configuring a Web Services Infrastructure .....</b>	<b>105</b>
Overview .....	105
Configure Web applications .....	106
<i>Creating Web Applications</i> .....	108
<i>Application Pools</i> .....	108
Manage Web sites .....	110
<i>Migrating and Upgrading to IIS 7</i> .....	110
<i>Configuring Sites and Virtual Directories</i> .....	111
Configure a File Transfer Protocol (FTP) server .....	113
Configure Simple Mail Transfer Protocol Services (SMTP) .....	114
Manage Internet Information Services (IIS) .....	115
Configure SSL security .....	117
Configure Web site authentication and permissions .....	119
Web Services in Windows Server 2008 R2 .....	121
<b>Practice Questions .....</b>	<b>122</b>
<b>Answers and Explanations .....</b>	<b>130</b>

## Abstract

This LearnSmart Exam Manual prepares candidates Microsoft Exam 70-649, Upgrading Your MCSE on Windows Server 2003 to Windows Server 2008, Technology Specialist. The manual was developed to provide candidates with every procedure, process and skill necessary to not only pass this exam but to make them competitive among other IT professionals.

Each of the exam's objectives is covered in-depth, beginning with Configuring Additional Active Directory Server Roles and ending with Configuring a Web Services Infrastructure. The manual's aim is to instruct, not confuse. For this reason, candidates will find visual aids and charts, as well as practice questions to test their ability to recall important concepts.

In addition, qualified candidates will be pleased to know that this exam manual was recently updated to include material related to Windows Server 2008 R2. Newly-added topics include Active Directory Server Roles and Windows Server 2008 R2, Server 2008 R2 Network Monitoring and Management, Hyper-V R2 and Windows Deployment for Windows Server 2008 R2.

## What to Know

Passing this Microsoft exam, Upgrading Your MCSE on Windows Server 2003 to Windows Server 2008, Technology Specialist (70-649), earns qualified candidates the following certifications: the Microsoft Certified Technology Specialist (MCTS): Windows Server 2008 Active Directory Configuration; the Microsoft Certified Technology Specialist (MCTS): Windows Server 2008 Network Infrastructure Configuration; and the Microsoft Certified Technology Specialist (MCTS): Windows Server 2008 Application Platform Configuration. In addition, passing this exam counts as credit towards the MCITP: Server Administrator and MCITP: Enterprise Administrator certifications. As one can expect, the exam is demanding as it is a composite of three stand-alone exams, Exams 70-640, 70-642 and 70-643, and tests candidates on a wide range of skills related to the core technology features of Windows Server 2008 R2 and builds upon skills previously validated by a Microsoft Certified Systems Engineer (MCSE) on Windows Server 2003.

The prerequisites for the exam are rigorous. The exam is aimed towards IT professionals who currently hold an MCSE on Windows Server 2003 and have at least one year of experience working in complex computing environments. Microsoft defines these computing environments as those having 250 to 5,000 or more users; three or more physical locations; three or more domain controllers; complex network services and resources; and vast connectivity requirements. As the MCSE is a prerequisite for the exam, no candidates can earn credit towards other certification unless they have earned the MCSE.

The official domains of this exam are:

- Configuring Additional Active Directory Server Roles
- Configuring IP Addressing and Services
- Monitoring and Managing a Network Infrastructure
- Deploying Servers
- Configuring Remote Desktop Services
- Configuring a Web Services Infrastructure

## Study Tips

As when taking any exam, preparation is everything. In most cases, reading only one book will not sufficiently prepare you for an exam as challenging as this exam. Therefore, in addition to knowing all aspects of the information presented in this manual, you will want to take advantage of all the other resources and exam preparation materials at your disposal.

For example, online video training allows you to customize your learning experience and absorb information at your own pace. You can watch video chapters as many times as necessary to understand particularly difficult concepts. Of course, unless you are especially good at retaining information you gather in a lecture environment, watching a video may not be enough.

When taking the actual exam, manage your time well. You should have more than enough time to complete the exam, but don't spend too much time on any one question. If you get stuck, return to the question at the end of the exam. If you're sufficiently prepared, you'll encounter many questions that seem easy. You want to make sure that you have time to answer all of the questions – easy and difficult – on the exam.

# Configuring Additional Active Directory Server Roles

## Active Directory Lightweight Directory Services – Background and Configuration

Active Directory Lightweight Directory Services (AD LDS) is a server role that provides centralized directory access and management using the Lightweight Directory Access Protocol, (LDAP). It provides authentication, directory data storage and allows query and retrieval of information by directory enabled applications, and does not require the “heavy” overhead of the Active Directory Domain Services (AD DS).

In Windows Server 2008 operating system, the AD LDS provides all the functionality that was provided by the Active Directory Application Mode (ADAM) in Windows Server 2003 and XP Professional. The AD LDS is optimized for speed of read access, and provides an optimized environment for integrating enterprise applications that require directory services, such as: line of business systems, customer relationship management systems, global information management systems and Human Resources Management applications. The AD LDS is primarily designed for use by applications, as a central directory store for information.

Windows 2008 does not require the deployment of domains or domain controllers, as required by Active Directory Domain Services. The same functionality will be provided by AD LDS, and can be used as a totally separate infrastructure for custom application deployment and development.

The following can be configured to run the AD LDS server role:

- Member Servers
- Domain Controllers
- Stand-alone Servers

AD LDS retains many of the functions of AD DS, including:

- Application directory partitions
- LDAP over SSL
- Support for the Active Directory API, or AD Services Interfaces
- Multi-master replication

AD LDS differs from AD DS in many ways, including the following:

- AD LDS does not support domains and forests
- AD LDS does not support Group Policy
- AD LDS does not support Global Catalogs
- AD LDS does not store security principals
- Windows cannot authenticate users stored in AD LDS, or use AD LDS users in Access Control Lists



There are many special considerations when implementing AD LDS:

- AD LDS is designed to be a provide directory services for applications, and the creation, management and removal of directory objects will be done through these applications.
- AD LDS does not support domain centric management tools such as Active Directory Users and Computers and Active Directory Domains and Trusts.
- AD LDS directories can be managed through the use of directory tools, such as:
  - **Ldp.exe** - is a support utility that provides the ability to search directories for information.
  - **ADSI Edit** - Can be used for creating, deleting, viewing and overall modification of objects within the directory.
  - Other schema and directory management utilities.

There are several instances where AD LDS is preferred over AD DS, and it should be considered in the following situations:

- When support is required for specific applications that have a limited scope of users.
- When distributed applications support a broad geographic user base, and data access is required in divers locations.
- When legacy applications require LDAP support.
- Specific applications rely on LDAP, and need high speed, local directory access.
- For external facing applications that reside within a perimeter network or DMZ.
- Applications that require extensive LDAP schema alterations.
- When a custom development environment for directory applications is required.

Before creating an AD LDS instance, you need to do a bit of planning, and preparation:

1. Create a data drive on the server. You need to place the directory stores on a drive that is separate from the operating system.
2. You will need to decide on a unique name for the instance, and this will identify the instance, and name all of the required files.
3. Create an administrative group for the AD LDS, typically a domain group.
4. Designate the application partition within Active Directory with a Distinguished Name (DN). The partition can be created in any one of 3 ways:
  - a. When you create the instance
  - b. When you install an application that is bound to the instance
  - c. Manually through an LDAP tool
5. Ensure the appropriate TCP/IP ports can be used through the service. Ad LDS uses the following port numbers:
  - a. 389 – Standard LDAP port
  - b. 636 – Secure LDAP

**Note:** These are the same ports used by AD DS. It is not recommended to have AD DS and AD LDS on the same server.

6. Create/Designate the AD LDS Service Account.
7. Create/Add any additional LDIF files required for the instance. Note: LDIF files are imported during the creation of the instance, and can set synchronization guidelines, create customizations and provide integration (to name a few). Below are some specific LDIF files and their purpose:
  - a. **MS-InetOrgPerson.ldf** – Contains the definition of the inetOrgPerson LDAP class.
  - b. **MS-User.ldf** – Contains all user classes and attributes.
  - c. **MS-ADLDS-DisplaySpecifiers.ldf** – this ldf is required for snap-in operations and is required if you plan to manage your instance with the Active Directory Sites and Services Snap-in.
  - d. **MS-adamschemaw2k3.ldf** – required if you are going to be synchronizing with Ad DS in Server 2003.
  - e. **MS-adamschemaw2k8.ldf** - required if you are going to be synchronizing with Ad DS in Server 2008.
  - f. **MS-AZMan.ldf** – supports the Windows Authentication Manager.

Below are the steps required to create a new LDS instance:

1. Click Start, go to Administrative Tools, and then click on Active Directory Lightweight Directory Services Setup Wizard, and click Next.
2. On the Setup Options page, click on “A unique instance,” and then click Next.
3. On the Instance Name page, provide a name for the AD LDS instance. This name will be used on the local computer to uniquely identify the AD LDS instance, and name the files and services associated with it.
4. On the Ports page, specify the communications ports that the AD LDS instance uses to communicate. AD LDS can communicate by using both LDAP (389) and Secure Sockets Layer (SSL) (636).
5. Within the “Application Directory Partition” step, you can create an application directory partition by clicking “Yes, create an application directory partition.” Or, you can select “No, do not create an application directory partition.” If you choose No, you must then create an application directory partition manually after the installation wizard.
6. On the “File Locations” page, you can change the default installation directories for the AD LDS data and recovery (log) files. By default, the AD LDS data and recovery files are installed in %ProgramFiles%\Microsoft ADAM\instancename\data.
7. Within the “Service Account Selection” page, you will select the service account for AD LDS. The AD LDS service will run under this account’s security context. Like most network services, the Active Directory Lightweight Directory Services Setup Wizard defaults to the Network Service account.

8. Select a user or group to become the default administrator for the AD LDS instance on the "AD LDS Administrators page." This user/group will have full administrative control of the AD LDS instance. By default, the Active Directory Lightweight Directory Services Setup Wizard specifies the currently logged on user.
9. On the "Importing LDIF Files" page, you can import schema LDAP Data Interchange Format (LDIF) files, and use them in the setup and operations of the instance.
10. The "Ready to Install" allows you an opportunity to review your installation selections. Click Next, and the Active Directory Lightweight Directory Services Setup Wizard copies files and sets up AD LDS on your computer. Click Finish when done.

## Directory Rights Management Service (AD RMS) – Background and Configuration

The Active Directory Rights Management Service provides a framework to create solutions to protect information. It works hand in hand with AD RMS-enabled applications to protect sensitive information by providing consistent usage policies and rights management for several content types including office documents, web sites, intranet content and email. Like many of the other enhancements in Windows Server 2008, it provides developers and applications the development hooks to add information protection functionality.

The AD RMS protects and manages information through the following elements:

- **Trusted Entities** – These entities can be specified, and include: applications, users, groups and computers that are a trusted part of an AD RMS system. These entities are then granted rights to specific content.
- **Usage conditions and rights** – Once trusted entities are established, they can then be assigned rights and conditions that specify how they can interact with specific rights protected content. Specific rights can include save, forward, read, write, copy print, etc. Along with rights, certain conditions can be specified that add an additional dimension to the control. An example of a condition would be a rights expiration date.
- **Encryption** – Encryption allows data to be locked through the use of an electronic key, and provides another level of validation of the trusted entity. Decryption of content by users with appropriate rights can be accomplished through the user of a browser or application that is AD RMS enabled.

There are several ways to implement AD RMS:

- **Internal use** – At its simplest, AD RMS is used to manage and protect the rights on internal documents. It can provide a vehicle to protecting content from unauthorized employee access, protect content that is copied to USB hard drives and even prevent unauthorized email distribution.
- **Internal and External use** – While AD RMS can be used just to protect information and content within an organization, it can also be used in sharing content with trusted partners and third parties. Once again, only privileges/rights authorized can be used on specific content.

The AD RMS provides a hierarchy of managed entities to provide persistence of policies across all managed entities:

- **AD RMS Deployment** – this is the overall process by which ADRMS is deployed across an organization.
- **AD RMS Web Services** – this provides a communication medium for computers within an AD RMS cluster.
- **AD RMS Logging Service** – this runs on each computer within a cluster running AD RMS and provides login information from which reports can be generated.

Server 2008 provides many new features that were absent in previous versions of the Windows Rights Management Services (RMS). The new features were added to extend the use of the service beyond your organization and ease the administrative overhead. The new features provided by 2008, include:

- **Microsoft Management Console (MMC) administrative interface** – earlier versions of RMS used a web interface, which was difficult to manage.
- **Installation** – The AD RMS is provided as a server role in 2008, providing simplified installation, and management. The server role automatically installs all required services, including message queuing and IIS.
- **AD RMS server self-enrollment** – the enrollment process is now all done locally, removing the requirement for having to connect to MS Enrollment Services.
- **Additional administrative roles that allow for responsibility delegation** – three new roles:
  - AD RMS Enterprise Administrators
  - AD RMS Template Administrators
  - AD RMS Auditors
- **Active Directory Federation Services (AD FS) integration** – AD FS allows organizations to collaborate with external entities with their rights-protected content without the need for AD RMS deployment in both locations.
- **AD RMS server role**

An AD RMS system performs the following processes, and includes client and server pieces:

- Creating rights templates and rights-protected files
  - Centralized templates can control usage, and provide a seamless and efficient way to standardize the application of privilege through policy.
- Licensing of rights-protected information
  - Provides a mechanism to issue certificates and identify trusted entities. Once trusted, a user/group/service can then publish rights protected content and assign rights to protect that content. These rights are then pervasive, and persist internally and externally.
- Licensing for the decryption of rights-protected content
  - Licenses can be issued to entities which are then interpreted, and applied to the content to provide adequate access.

When deploying the AD RMS, there are a few special considerations which must be taken in to account:

- The AD RMS requires the Active Directory Domain Service to provide authorization for users attempting to access rights-protected content.
- User accounts that are used to register the AS RMS service connection point require special write access to the AD DS Service Container.
- In production environments, due to the high logging requirements, the configuration and logging information for AD RMS should be stored in a separate database server. (Note, in the install process, the Windows internal DB will be used unless another DB is specified).

The new AD RMS Administrative roles provide the ability to delegate control of the environment, and provide built in access level control:

- **AD RMS Administrator Role** – provides management of all AD RMS setting and policies. By default this will include local administrators and the account that installs the service.
- **AD RMS Template Administrators** – these users can manage rights policy templates, and can list and read all policy templates, modify existing templates and export templates as well.
- **The AD RMS Auditors** - role is a read only account that can be used to read information, logs and run reports.

AD RMS operation are driven by client content creation, and consist of the AD RMS Client which communicates with the Active Directory Domain Services. The AD DS provides a management interface, as well as authentication services and access control – who and what can access the AD RMS. There are several components beyond the mentioned that comprise the overall AD RMS infrastructure:

- The server that houses the AD RMS Server role, and provides certificate and licensing management.
- The database that contains the AD RMS configuration and logging information. This can be a Windows Internal Database, or SQL Server.
- An IIS 7 Web server to provide web services.
- The AD DS directory provides an administrative interface, and authentication.
- Transaction coordinating and distributed services are provided through the Message Queuing service.

You can well imagine that a complex rights management system has many pre-requisites to ensure seamless operations and minimal issues. Below are the installation requirements:

- You will need to enable the role on a 2008 member server and can be enabled on any platform with the exception of 2008 Web.
- The installation/service account must be part of the domain and have local administrative privileges. Ensure that the account also has access to the SQL server, if using this database storage method, and that it has read access to AD DS.
- The AD RMS role must be enabled on a member server within the same forest, within Active Directory Domain Services, as the user accounts that will be using the service and accessing content.

- Access the server through a DNS name (CNAME record). This is always a best practice for application servers, as it provides an easy way to redirect traffic if you ever switch physical servers. If using a cluster, specify a separate record for the cluster URL, and a separate record for the DB host computer. Never use local host in the URL.
- Obtain an SSL certificate from a trusted certificate authority for the production environment. You may use self-signed certificates for test, but never use them in production.
- You can use the Windows Internal Database for test environments, but never use in production as it does not support remote connections. SQL is recommended for all production environments.

Setting up the ADRMS Infrastructure is a 3 step process:

1. Setting up the infrastructure
  - a. Configure the domain controller
  - b. Configure the AD RMS Database
  - c. Configure the AD RMS Root Cluster
  - d. Configure the AD RMS Client
2. Installing and Configuring AD RMS role
3. Verifying operations on the client

In AD RMS, trusted connections are established and maintained through a set of different certificates or licenses. They are described in the table below:

Certificate/License	Description/Purpose	Content
Server Licensor Certificate (SLC)	This self-signed certificate is generated when you establish the first server role in the cluster. Other servers in the root cluster will share this certificate.	The server public key
Client Licensor Certificate (CLC)	This certificate is sent to a client application when requested, and is tied to the RAC of the user. This is sent when online, and provides the ability to publish content when not connected to the organizations network.	-Client licensor public key -Client licensor private key -Public key of the issuing cluster
Machine Certificate	This certificate is established on the client computer the first time an application communicates with Ad RMS.	-Public key of the device/computer -Private key of the computer is held within a "lockbox"
Rights Account Certificate (RAC)	This is provided to the user whenever they initially open rights-protected content, and is a user's identity within the overall AD RMS system. The RAC is established for the specific user account credentials on a specific device, and is valid for a default time of a year.	-Public key of the user -Private key of the user (encrypted with device public key)
Use License	Provides the authenticated user with specific rights on protected content. Must have the RAC to access content.	-Content key encrypted with user public key
Publishing license	Whenever a user publishes rights-protected content, this key is created. It specifies conditions, rights and users.	-Content key, encrypted with server public key

**Figure 1:** Certificates and Licenses

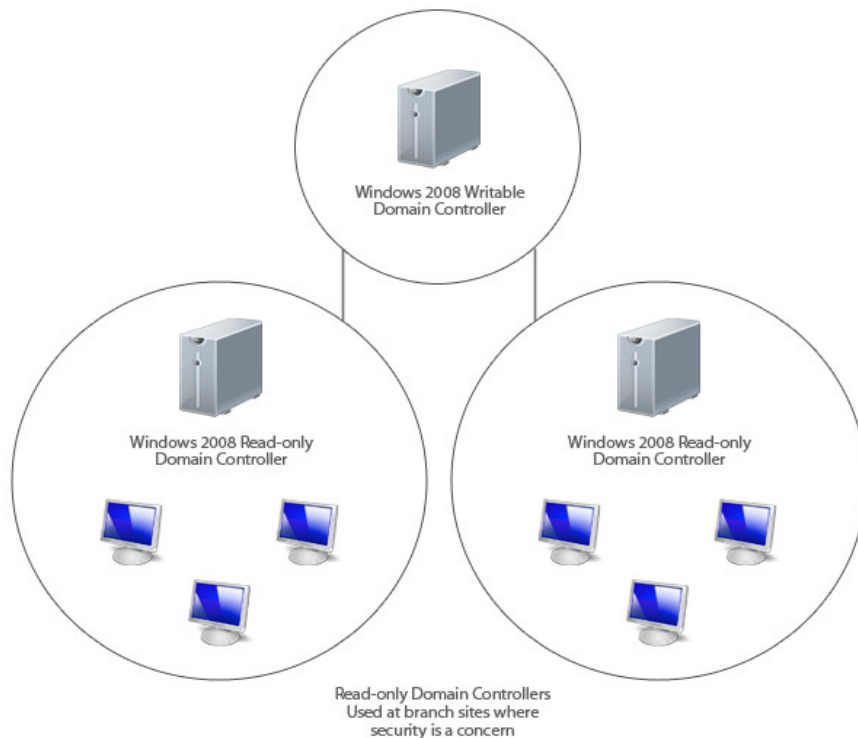
## Read Only Domain Controller (RODC) – Background and Configuration

Windows Server 2008 provides a new type of domain controller: the Read Only Domain Controller (RODC). This new controller type is primarily an addition to the enhanced security features of the new OS, and provides organizations a way to deploy a domain controller in areas that cannot be guaranteed physical security. The RODC hosts only certain partitions of the Active Directory Domain Service, which are read-only. Primarily for branch office deployments, the RODC provides logon capabilities at remote locations without the requirement of passing traffic over a Wide Area Network connection to authenticate to centralized domain controllers, and allows partitioning of the physical infrastructure through logical means. The RODC can also be used for external and/or extranet applications. Note: RODC deployment requires a Windows 2008 Domain controller. The primary benefits of deploying a RODC at a remote location are:

- Improved security and integrity of domain information without the ability to write to the domain
- Reduced logon times due to a local domain controller, providing fast reliable access without WAN traffic
- Overall efficiency with regards to network resource access

The RODC is primarily designed to be deployed at sites with the following characteristics:

- Few users
- Poor connectivity or bandwidth to a central site
- Inadequate physical security
- No local IT staff



**Figure 2:** Read-Only Domain Controllers

The RODC includes functionality that improves overall functions at locations with the above characteristics through the following feature set:

- An Active Directory Domain Service that is read only
  - ▶ The RODC holds all of the Active Directory objects and attributes typically found in a full domain controller, with the exception of account passwords. Changes cannot be made to the domain database on the RODC, and must be performed on a writable domain controller, and then replication to the RODC.
  - ▶ Filtered attribute sets provide the ability to filter replicated data structures so passwords, encryption keys and credentials for applications that use the AD database as storage can be protected.
  - ▶ Filters are configured on the schema operations master (the server that holds this role).
- One way or unidirectional replication with full domain controllers
  - ▶ Changes cannot originate at the RODC.
  - ▶ Both AD DS and Directional File System (DFS) SYSVOL replication are unidirectional.
  - ▶ All other DFS replication of RODC shares is bidirectional.
- The caching of credentials
  - ▶ By default the RODC does not store all computer or user credentials.
  - ▶ There are two exceptions: the RODC computer account and a special `krbtgt` account used by the RODC in operations.
  - ▶ RODCs only cache credentials of users who have authenticated to the RODC, minimizing risk of exposure.
- Separation of Administrator Roles
  - ▶ Branch users can be delegated local administrative rights on the RODC.
- A Domain Name System (DNS) that is also read only
  - ▶ The RODC can run DNS and provide lookups for local users through a read only `ForestDNSZones` and `DomainDNSZones`.



## Active Directory Federation Services (ADFS) – Background and Configuration

Active Directory Federation Services (ADFS) provides identity access to Internet browsers, of both internal and external clients, through a single sign on. The clients can be in different networks, and even different organizations providing seamless access to partners and third parties. ADFS solves the existing issue of multiple credentials to access web applications that are not housed within your network/organization, and allows secure credentialing across the Internet. Deploying federation servers within partners is accomplished through the designation of two separate organization types:

- **Resource Organization** – These entities manage their own resources that are accessible from the outside, and usually deploy either AD FS web servers or ADFS federation servers to manage specific resources for their trusted partners and other third parties.
- **Account Organization** – These entities own and manage their user accounts and provide federation servers that provide authentication for their own local user base. These servers then create tokens that federation servers within the above mentioned resource organization to authorize users.

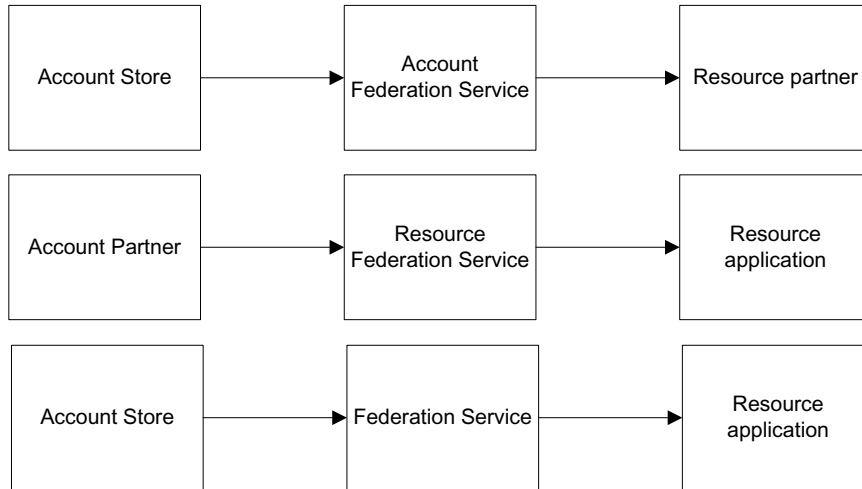
The AD FS server role provides the following services:

- **Federation Service Proxy** – AD FS relies on a proxy that is in the perimeter network/DMZ and relays authentication requests to the federation server. WS – Federation Passive Requester Profile protocols (WS-FPRP) are used by the federation service proxy to interact with browser clients, and collect user authentication information. The credentials are then relayed to the federation service.
- **Federation Service** – Federation servers route authentication requests from users, located anywhere. The Federation Service can be comprised of any number of servers that share a common trust policy and provide the mentioned authentication services.
- **Claims-aware agent** – The claims aware agent is used by claim-aware applications running on web servers and provide the ADFS security token query services. The claims process is what enables user authentication, and determine user access to applications.
- **Windows token-based agent** - This agent provides conversion services, and converts AD FS tokens into windows NT access tokens for applications that require windows based authentication.

AD FS uses three different types of components to facilitate access:

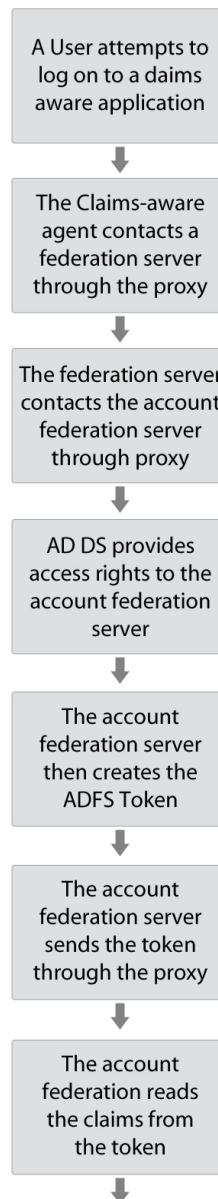
- **Claims** – Claims are used for authorization purposes, and are statements made about users that house information about name, key, privilege, capability, etc. The ADFS is a broker for claims that are then translated into decisions for access.

The FS facilitates three different types of communication flows:



**Figure 3:** Communication Flows

- **Cookies** - The AD FS uses three types of cookies.
  - ▶ **Authentication Cookies** – are issued by the FS or ADFS Web Agents, and stores security tokens in cookies. The Authentication cookie is used to facilitate single sign on, and is written to the client once upon access. Once the cookie is stored, it is used for any subsequent authentication.
  - ▶ **Sign Out Cookie** – resource partner and target servers use these cookies to “clean up” any cache or artifacts after client sign off.
  - ▶ **Account Partner Cookie** – This cookie is used to store client account partner information, after the information is discovered through the FS. It eliminates unnecessary discovery of information.
- **Certificates** – AD FS uses certificates to encrypt data transfers. Token-signing and server authentication certificates are used to facilitate the entire process.



**Figure 4:** Certificates

Windows Server 2008 ADFS provides enhancements that extend support and ease the administrative burden of managing FS:

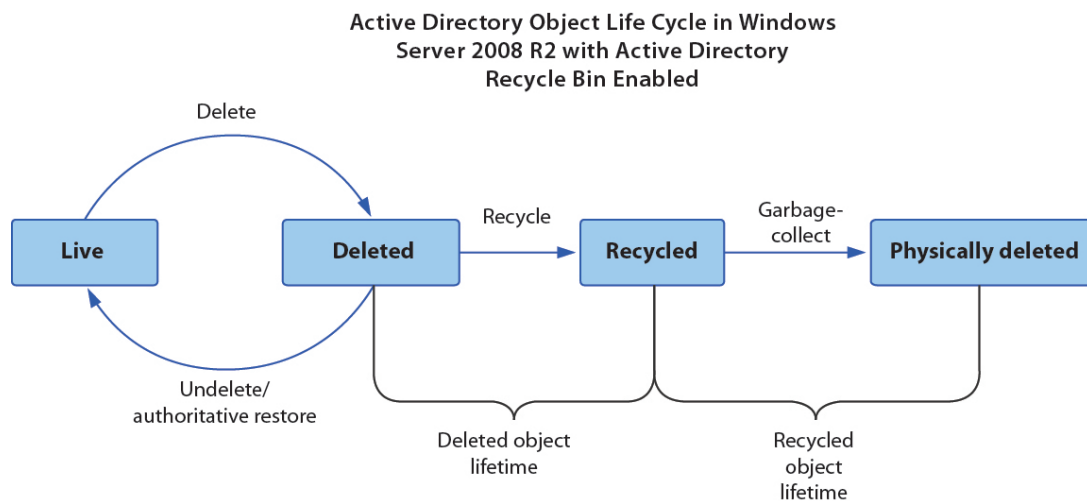
- **Improved installation** – in 2003, you had to add ADFS through the Add Program s interface. In 2008, this is accomplished by assigning a server role using the server manager. Microsoft has provided a configuration wizard to simplify the config process, and automatically install dependencies and services required to run the service. This includes the web server role, and also ASP.NET 2.0.

- **Enhanced application support** – Server 2008 and ADFS have improved the overall application integration, especially in regards to SharePoint and AD RMS.
  - The main advantage from a Sharepoint perspective is the single sign on capabilities, and the option to configure SharePoint as a claims-aware application. This allows for role-based access control and the administration of sites and membership through ADFS.
  - The integration of AD RMS and AD FS allows organizations to collaborate on rights-managed content facilitated through the use of existing federated trust relationships between their partners.
- **Ease of Administration of federated trusts** – Server 2008 provides enhanced import and export capabilities surrounding policy files. The policies can be exported to an xml files, and sent to partner administrators that can simply import to establish trust relationships. The policy file provides all the necessary components to create the trust.

## Active Directory Server Roles and Windows Server 2008 R2

Windows Server 2008 R2 servers acting as domain controllers (DCs) continue to support the features and capabilities covered in this section up to this point; however, they also add several new features and tools. You should be aware of the following new features as you prepare for exam 70-649:

- **Active Directory Recycle Bin**  
The Active Directory Recycle Bin allows administrators to easily recover deleted objects. Earlier versions of Active Directory supported recovery of deleted objects through the use of Windows Server Backup or through tombstone reanimation. Both processes were difficult and possibly time consuming. With the new Active Directory Recycle Bin, you can restore and object with its required linked valued (for example groups that may have also been deleted). The Active Directory Recycle Bin is disabled by default and the forest functional level must be set to Windows Server 2008 R2 to enable it. Once enabled, the Recycle Bin may not be disabled. The following image illustrates the life cycle of an Active Directory object when the Recycle Bin is enabled.



**Figure 5:** Active Directory Object Life Cycle

- **Windows PowerShell Enhancements**

Windows Server 2008 R2 provides a much improved Active directory module for Windows PowerShell. The Active Directory module can be used to map a domain to a provider drive so that you can browse through the domain as if it were a folder structure on a disk drive. In addition, the Active Directory cmdlets, listed in the following table:

Cmdlet Name	Purpose of Cmdlet
<b>Disable-ADAccount</b>	Disables an Active Directory account.
<b>Enable-ADAccount</b>	Enables an Active Directory account.
<b>Search-ADAccount</b>	Gets Active Directory user, computer, and service accounts.
<b>Unlock-ADAccount</b>	Unlocks an Active Directory account.
<b>Get-ADAccountAuthorizationGroup</b>	Gets the Active Directory security groups that contain an account.
<b>Set-ADAccountControl</b>	Modifies user account control (UAC) values for an Active Directory account.
<b>Clear-ADAccountExpiration</b>	Clears the expiration date for an Active Directory account.
<b>Set-ADAccountExpiration</b>	Sets the expiration date for an Active Directory account.
<b>Set-ADAccountPassword</b>	Modifies the password of an Active Directory account.
<b>Get-ADAccountResultantPasswordReplication Policy</b>	Gets the resultant password replication policy for an Active Directory account.
<b>Get-ADComputer</b>	Gets one or more Active Directory computers.
<b>New-ADComputer</b>	Creates a new Active Directory computer.
<b>Remove-ADComputer</b>	Removes an Active Directory computer.
<b>Set-ADComputer</b>	Modifies an Active Directory computer.
<b>Add-ADComputerServiceAccount</b>	Adds one or more service accounts to an Active Directory computer.
<b>Get-ADComputerServiceAccount</b>	Gets the service accounts that are hosted by an Active Directory computer.
<b>Remove-ADComputerServiceAccount</b>	Removes one or more service accounts from a computer.
<b>Get-ADDefaultDomainPasswordPolicy</b>	Gets the default password policy for an Active Directory domain.
<b>Set-ADDefaultDomainPasswordPolicy</b>	Modifies the default password policy for an Active Directory domain.
<b>Move-ADDirectoryServer</b>	Moves a domain controller in AD DS to a new site.
<b>Move-ADDirectoryServerOperationMasterRole</b>	Moves operation master (also known as flexible single master operations or FSMO) roles to an Active Directory domain controller.
<b>Get-ADDomain</b>	Gets an Active Directory domain.
<b>Set-ADDomain</b>	Modifies an Active Directory domain.

<b>Get-ADDomainController</b>	Gets one or more Active Directory domain controllers, based on discoverable services criteria, search parameters, or by providing a domain controller identifier, such as the NetBIOS name.
<b>Add-ADDomainControllerPasswordReplicationPolicy</b>	Adds users, computers, and groups to the Allowed List or the Denied List of the read-only domain controller (RODC) Password Replication Policy (PRP).
<b>Get-ADDomainControllerPasswordReplicationPolicy</b>	Gets the members of the Allowed List or the Denied List of the RODC PRP.
<b>Remove-ADDomainControllerPasswordReplicationPolicy</b>	Removes users, computers, and groups from the Allowed List or the Denied List of the RODC PRP.
<b>Get-ADDomainControllerPasswordReplicationPolicyUsage</b>	Gets the resultant password policy of the specified ADAccount on the specified RODC.
<b>Set-ADDomainMode</b>	Sets the domain functional level for an Active Directory domain.
<b>Get-ADFineGrainedPasswordPolicy</b>	Gets one or more Active Directory fine-grained password policies.
<b>New-ADFineGrainedPasswordPolicy</b>	Creates a new Active Directory fine-grained password policy.
<b>Remove-ADFineGrainedPasswordPolicy</b>	Removes an Active Directory fine-grained password policy.
<b>Set-ADFineGrainedPasswordPolicy</b>	Modifies an Active Directory fine-grained password policy.
<b>Add-ADFineGrainedPasswordPolicySubject</b>	Applies a fine-grained password policy to one more users and groups.
<b>Get-ADFineGrainedPasswordPolicySubject</b>	Gets the users and groups to which a fine-grained password policy is applied.
<b>Remove-ADFineGrainedPasswordPolicySubject</b>	Removes one or more users from a fine-grained password policy.
<b>Get-ADForest</b>	Gets an Active Directory forest.
<b>Set-ADForest</b>	Modifies an Active Directory forest.
<b>Set-ADForestMode</b>	Sets the forest mode for an Active Directory forest.
<b>Get-ADGroup</b>	Gets one or more Active Directory groups.
<b>New-ADGroup</b>	Creates an Active Directory group.
<b>Remove-ADGroup</b>	Removes an Active Directory group.
<b>Set-ADGroup</b>	Modifies an Active Directory group.
<b>Add-ADGroupMember</b>	Adds one or more members to an Active Directory group.
<b>Get-ADGroupMember</b>	Gets the members of an Active Directory group.
<b>Remove-ADGroupMember</b>	Removes one or more members from an Active Directory group.
<b>Get-ADObject</b>	Gets one or more Active Directory objects.

<b>Move-ADObject</b>	Moves an Active Directory object or a container of objects to a different container or domain.
<b>New-ADObject</b>	Creates an Active Directory object.
<b>Remove-ADObject</b>	Removes an Active Directory object.
<b>Rename-ADObject</b>	Changes the name of an Active Directory object.
<b>Restore-ADObject</b>	Restores an Active Directory object.
<b>Set-ADObject</b>	Modifies an Active Directory object.
<b>Disable-ADOptionalFeature</b>	Disables an Active Directory optional feature.
<b>Enable-ADOptionalFeature</b>	Enables an Active Directory optional feature.
<b>Get-ADOptionalFeature</b>	Gets one or more Active Directory optional features.
<b>Get-ADOrganizationalUnit</b>	Gets one or more Active Directory OUs.
<b>New-ADOrganizationalUnit</b>	Creates a new Active Directory OU.
<b>Remove-ADOrganizationalUnit</b>	Removes an Active Directory OU.
<b>Set-ADOrganizationalUnit</b>	Modifies an Active Directory OU.
<b>Add-ADPrincipalGroupMembership</b>	Adds a member to one or more Active Directory groups.
<b>Get-ADPrincipalGroupMembership</b>	Gets the Active Directory groups that have a specified user, computer, or group.
<b>Remove-ADPrincipalGroupMembership</b>	Removes a member from one or more Active Directory groups.
<b>Get-ADRootDSE</b>	Gets the root of a domain controller information tree.
<b>Get-ADServiceAccount</b>	Gets one or more Active Directory service accounts.
<b>Install-ADServiceAccount</b>	Installs an Active Directory service account on a computer.
<b>New-ADServiceAccount</b>	Creates a new Active Directory service account.
<b>Remove-ADServiceAccount</b>	Remove an Active Directory service account.
<b>Set-ADServiceAccount</b>	Modifies an Active Directory service account.
<b>Uninstall-ADServiceAccount</b>	Uninstalls an Active Directory service account from a computer.
<b>Reset-ADServiceAccountPassword</b>	Resets the service account password for a computer.
<b>Get-ADUser</b>	Gets one or more Active Directory users.
<b>New-ADUser</b>	Creates a new Active Directory user.
<b>Remove-ADUser</b>	Removes an Active Directory user.
<b>Set-ADUser</b>	Modifies an Active Directory user.
<b>Get-ADUserResultantPasswordPolicy</b>	Gets the resultant password policy for a user.

Figure 6: PowerShell Enhancements

- **Active Directory Administrative Center (ADAC)**

The ADAC is a new tool for Active Directory object management. Using this tool you can create and manage new user accounts, groups, computer accounts and organizational units. The following image shows the ADAC interface:

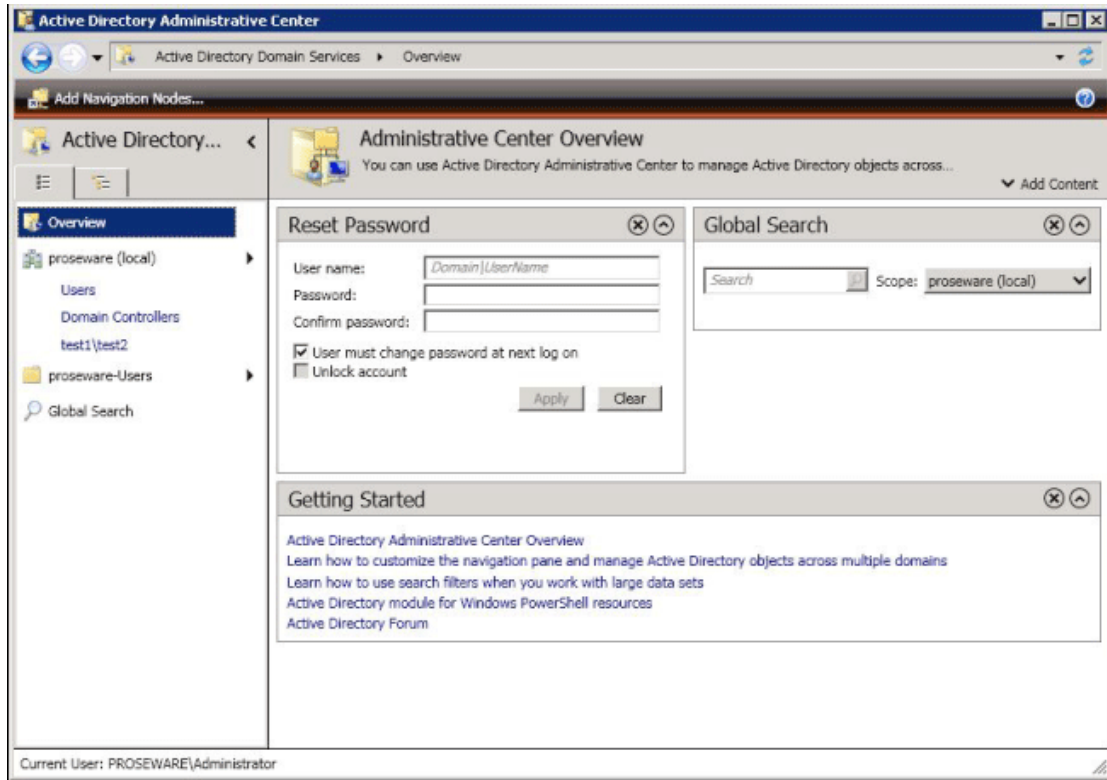


Figure 7: ADAC

- **Active Directory Best Practices Analyzer (BPA)**

The Active Directory BPA is new to the Server Manager in Windows Server 2008 R2. The BPA will scan your Active Directory installation on the server and locate any areas outside of best practices. The BPA will verify several Active Directory configuration settings including:

- ▶ DNS accessibility
- ▶ Operations master (FSMO) connectivity
- ▶ Number of domain controllers in the domain (at least two functioning)
- ▶ Required services are operational
- ▶ Replication configuration is appropriate in that each site contains a global catalog server
- ▶ The PDC emulator operations master is configured to synchronize time with a valid time source
- ▶ All virtualized domain controllers run on Hyper-V and not another platform
- ▶ Active Directory has been backed up within the last 8 days



- Active Directory Web Services (ADWS)**  
 ADWS is a new Windows Server 2008 R2 service that establishes a Web service interface to the Active Directory domains. Client applications such as the Active Directory Module for Windows PowerShell and ADAC require ADWS. ADWS is installed automatically when you add the AD DS or AD LDS server roles to a Windows Server 2008 R2 server. ADWS requires that TCP port 9389 be open on the domain controller where it is running. The ADWS functions can be provided for earlier version domain controllers, such as Windows Server 2003 with SP2 or Windows Server 2003 R2 with SP2, by downloading and installing the Active Directory Management Gateway Services (AD MGS). AD MGS allows the PowerShell module and ADAC to function against these earlier versions of Active Directory.
- Authentication Mechanism Assurance**  
 Many environments require that users authenticate with certificates (typically with smart cards) when accessing sensitive information; however, they may allow them to authenticate with user names and passwords for normal operations. This was difficult to configure with earlier versions of Active Directory. Windows Server 2008 R2 introduces authentication mechanism assurance, which allows users to become members of specific groups only when they authenticate with a certificate. In such a scenario, the user will have access to some resources only when she logs onto the network with her smart card.

## Offline Domain Join

The new offline domain join feature allows computers to join the domain without network connectivity. This is useful when initially installing client computers that may not have an always on network connection. Offline domain join requires that a metadata set be created for the client computer using the `djoin.exe /provision` command. On the destination client computer, you use the `djoin.exe /requestODJ` command to insert the metadata into the Windows directory. Once the data is inserted, the computer will be joined to the domain even if network connectivity is unavailable. This feature works only for Windows Server 2008 R2 and Windows 7 target computers. It may benefit administrators by allowing remote installations of Read-Only Domain Controllers (RODCs) before the WAN connections are available.

## Configuring IP Addressing and Services

### Configure IPv4 and IPv6 addressing

As a network professional, you should be very familiar with IPv4 addressing, and all the terminology. Below is a quick network addressing review.

An IPv4 address is a 32 bit address with a 32 bit subnet mask that divides the address into a network and host portion. With the depletion of addresses from the “public” address pool, the networking community has begun to implement several measures to use the space more efficiently, and move away from “classful” addressing.

- Classful Address Space** – the original IP address space was divided into the classes defined below:

Class	Range	Subnet Mask	Beginning of First Octet In binary
A	1-126	255.0.0.0	0
B	128-191	255.255.0.0	10
C	192-223	255.255.255.0	110
D (Multicast)	224-239	255.255.255.240	1110
E	240-255	Reserved	11110

Figure 8: Address Space

- **Subnetting** – the default IP address space is very inefficient and in most cases, addresses are wasted, or not used. Subnetting allows “borrowing” of bits the host portion of the address to define additional networks. Addresses have two sections: network, and host. The network segment is determined by the subnet mask. Variable Length Subnet Mask (VLSM) is a technique in which the subnet mask is adjusted in order to segment a given network. An example is below:

Network	195.1.1.0
Original Mask	255.255.255.0 (/24)

The network administrator has a network with 5 hosts, and does not want to waste addresses. To save on address space, the mask is adjusted:

New Network	195.1.1.0
New Mask	255.255.255.248 (/29)
New Mask Binary	11111111.11111111.11111111.11111000

This leaves 3 bits for the hosts, and using the equation  $2^n - 2$ , this gives us 6 host addresses to use.

$$2^3 - 2 = 6$$

We subtract 2 because the first address is used as the network address, and the last for the broadcast address (in this case 195.1.1.7). Completely dividing the network with this scheme will give us 32 subnets with 6 hosts each. How do you get the 32 subnets?

$$2^5 = 32 \quad \text{The five signifies the host bits borrowed.}$$

IP version 6 was created due to concerns over the rapid depletion of the IPv4 address space. The internet boom in the late 90s early 2000s consumed a large portion of the entire space. With the introduction of Network Address Translation, the concern slowed down, and the need for additional addresses has waned. Nonetheless, many improvements have been added to the standard. The benefits of IPv6 over IPv4:

- **Larger address space** - IPv4 provided  $2^{32}$  bits, whereas IPv6 provides  $2^{128}$  bits for addressing.
- **Better Security** – Ipv4 provided communication protection through IP security, or IPSec, which was an optional requirement by the standard, and was implemented quite differently by different manufacturers. IPv6 security is a requirement in the standard, and provides for better standardization across vendors.
- **Mobility** – the standard provides for a “sticky” address, which enables the network node to be reachable, no matter what its location. This transportable or mobile addressing provides for great flexibility on network connectivity options.
- **Integrated Quality of Service (QOS)** – QOS is required for latency sensitive application like voice and video. The IPv6 header provides information on how flow is handled.

## IPv6: Syntax

The IPv6 address is a 128 bit address that has been divided at 16 bit boundaries, with each 16 bit boundary converted to 4 digit hexadecimal. The format is called colon hexadecimal, because each 16 bit section is separated by a colon. The format of an address is below:

XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX

The IPv6 addresses ranges from 0000:0000:0000:0000:0000:0000:0000:0000 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.

In addition to this preferred format, IPv6 addresses may be specified in two other shortened formats:

- **Omit leading zeros**  
You can specify IPv6 addresses by omitting the leading zeros. For example, IPv6 address 1100:0000:0000:0000:0005:0600:300c:326b may be written as 1100:0:0:5:600:300c:326b.
- **Double colon**  
You can also specify IPv6 addresses by using double colons (::) in place of any series of zeros. IPv6 address ff06:0:0:0:0:c3 may also be written as ff06::c3. Double colons may be used only once within an IPv6 address.

Also, an alternate format for the IPv6 addresses merges the colon and dotted notation, so the IPv4 address may be embedded within an IPv6 address. Hex values are then specified for the left-most 96 bits, and the IPv4 decimal values are specified for the right-most 32 bits. This format insures IPv6 to IPv4 compatibility between nodes when you are working in a mixed network environment.

Here are the two types of IPv6 addresses that use this alternate format:

1. **IPv4-mapped IPv6 address**  
Used to represent IPv4 nodes as IPv6 addresses. This allows IPv6 applications to effectively communicate directly with IPv4 applications. For example, 0:0:0:0:ffff:192.1.56.10 and ::ffff:192.1.56.10/96 (shortened format).
2. **IPv4-compatible IPv6 address**  
Used for tunneling, and it allows IPv6 nodes to communicate effectively across an IPv4 network infrastructure. For example, 0:0:0:0:0:192.1.56.10 and ::192.1.56.10/96 (shortened format).

## IPv6: Address Types

**Unicast** – packets are delivered to a single interface. There are several different types of unicast addresses:

- **Global** – the global unicast address is equivalent to the IPv4 public address, and can be reachable anywhere on the internet. The key here is that the address is unique, and a set of addresses can be aggregated into a set space to provide a more efficient network/internet routing scheme. The structure of the unicast global address is broken down into three sections:
  - ▶ **Public Topology** – first 3 bits is the format prefix of 001. The next 13 bits are assigned by IANA, and is known as the Top Level Aggregation Identifier (TLA ID), and are assigned to large ISPs for distribution (additional 8 bits reserved for expansion). The next 24 bits are the Next Level Aggregate. ID (NLA ID) which is assigned to the customer site.
  - ▶ **Site Topology** – 16 bits that allow subnetting of an individual organization site. This is assigned to the site.
  - ▶ **Interface ID** – 64 bits for the interface node on a specific subnet.
- **Site-local** – these addresses are equivalent to private IPv4 addresses, and are for internal use only and cannot be routed over the internet. The sit-local and global unicast addresses share the same structure after the first 48 bits. Structure below:
  - ▶ The First 48 bits is fixed.
  - ▶ Subnet ID is 16 bits for use in internal subnetting.
  - ▶ Interface ID is 64 bits for individual address assignment.

- **Link-local** – these are similar to Automatic Private IP Addressing (APIPA) addresses found in IPv4, and hosts on the same subnet/link can communicate with each other on these addresses. The Neighbor Discovery process will provide address resolution. The first 64 bits of this address are fixed, and designated by FE80::/64. The last 64 bits, is once again the interface ID.
- **Unspecified** – designated by 0:0:0:0:0:0:0 or :: (double colon).
- **Unicast Loopback** – the equivalent of IPv4 127.0.0.1, but 0:0:0:0:0:0:1 or ::1.
- **Unicast 6to4** – used to establish communications between an IPv6 and v4 host over the internet, and is designated by 2002::/16.
  - ▶ First 16 bits are set.
  - ▶ Next 32 bits are the IPv4 address.
  - ▶ 16 bit SLA ID.
  - ▶ 64 bit Interface ID.
- **ISATAP Address** - This address provides IPv6 to IPv4 communication over an intranet.
  - ▶ 64 Bit Subnet prefix.
  - ▶ 32 bit ISATAP ID - 0000:5EFE.
  - ▶ 32 bit IPv4 address.

Examples:

With link-local prefix	FE80::5EFE:131.107.129.8
With site-local prefix	FECO::1111:0:5EFE:131.107.129.8
With global prefix	3FFE:1A05:510:1111:0:5EFE:131.107.129.8
With global 6to4 prefix	2002:9D36:1:2:0:5EFE:131.107.129.8

*Examples from MS IPv6 Tutorial*

**Multicast** – this address type provides the ability to send packets to multiple interfaces with a single transmission. They are similar to IPv4 multicast packets.

- The structure of the multicast address is as follows:
  - ▶ An 8 bit field – 1111 1111 that designates the multicast type.
  - ▶ A 4 bit flag section that can be 0 or 1 to designate the transient status.
  - ▶ A 4 bit scope, that designates whether it is interface local, link-local, site-local or global.
  - ▶ Group ID of 112 bits.

**Anycast** – This address type will route packets to the nearest interface (in terms of routing distance). These addresses are only assigned to routers and are only used as a destination address.

## IPv6: Implementing Compatibility

IPv6 implements several transition technologies to assist in the transition from IPv4 to IPv6.

- **IPv4 compatible addresses** – 0:0:0:0:a.b.c.d is used by systems that are compatible with both TCP/IP stacks to enable inter-technology communication.
- **IPv4 Mapped Addresses** – 0:0:0:0:ffff:a.b.c.d allows you to map an IPv4 node to an IPv6 address.
- **Teredo** - Teredo is an address assignment and automatic tunneling scheme that provides unicast IPv6 communications capability across the IPv4 Internet. 6to4, another automatic tunneling technology, works well when a 6to4 router exists at the edge of the network. A 6to4 router would use a public IPv4 address to build the 6to4 prefix and then would act as an IPv6 advertising/forwarding router. The 6to4 router encapsulates/decapsulates IPv6 traffic that is sent to and from specific site nodes. Unfortunately, 6to4 relies on public addressing, and has many issues with Network Address translation.

Teredo resolves this issue by allowing automotive IPv6 tunneling between hosts that are using Network Address Translation. The technology leverages UDP messages to communicate and translate multi-layer NATs. The Teredo infrastructure consists of several components:

- ▶ Clients - this is an IPv6/IPv4 node that supports a teredo tunneling interface, and sends information to another client or node.
- ▶ Servers – the server's primary role is to work with the clients and assist in the address configuration. The server runs on port UDP 3544.
- ▶ Relays - the relay is an IPv4/IPv6 router that relays packets from clients to the internet.
- ▶ Host Specific Relays – any communication between a teredo host and an IPv6 host must go through a relay.

The Teredo address format is specified below:

- First 32 bits are a Teredo specific prefix which is the same for all addresses: 2001::/32.
- Next 32 bits is the IPv4 address.
- There are 16 bits used to designate the type of NAT the client is within and a randomly generated number.
- The next 16 bits store what is called an obscured external port, or UDP port for mapping the connection. The port is obscured using an XOR operation.
- The last 32 bits is an obscured external address.

## IPv6: Tools

There are many tools you can use to troubleshoot and test the IPv6 configurations within your network. In Windows 2008, all the standard command line tools for testing connectivity have full IPv6 functionality: ping, pathping, ipconfig, tracert, netstat, route.

Windows has provided a new command shell for providing specific IPv6 operations, and it is used by typing netsh at the command prompt. Below are some sample commands:

- Netsh /? Will give you all the options. You can also use netsh /<option> /? To give you specific command syntax.
- Netsh interface ipv6 show addresses.

```

Administrator: C:\Windows\system32\cmd.exe
show teredo - Shows Teredo state.
show udpstats - Displays UDP statistics.
C:\Users\sboals>netsh interface ipv6 show addresses
Interface 1: Loopback Pseudo-Interface 1
Addr Type DAD State Valid Life Pref. Life Address
-----
Other Preferred infinite infinite ::1
Interface 11: Wireless Network Connection
Addr Type DAD State Valid Life Pref. Life Address
-----
Other Preferred infinite infinite fe80::c09:b8cc:7aa9:76e0%11
Interface 10: Local Area Connection
Addr Type DAD State Valid Life Pref. Life Address
-----
Other Deprecated infinite infinite fe80::7d3f:2c3f:5596:19ac%10
Interface 25: Local Area Connection* 12
Addr Type DAD State Valid Life Pref. Life Address
-----
Other Deprecated infinite infinite fe80::5efe:192.168.50.103%25
Interface 34: Local Area Connection* 23
Addr Type DAD State Valid Life Pref. Life Address
-----
Other Deprecated infinite infinite fe80::5efe:192.168.1.202%34
C:\Users\sboals>

```

Figure 9: Netsh interface

- Netsh interface ipv6 show dnsservers.

Note that the netsh can also be used to configure a wide variety of networking options, including interface settings, dhcp, dns, etc.

## IPv6: Configuration

There are two ways to configure IPv6 on an interface, you can manually set the interface IP through the properties dialog in the Local Area connection properties.

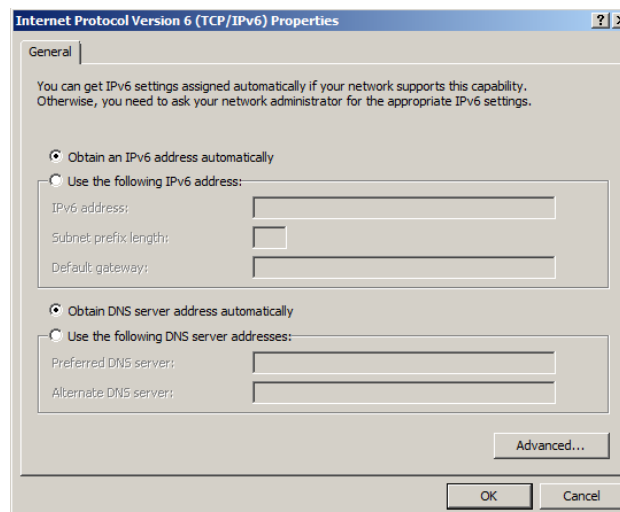


Figure 10: IPv6 Properties

You may also configure an interface and all properties through the use of the netsh command. Below are some commonly used commands:

**Set interface to DHCP:** *netsh interface ip set address "Local Area Connection" dhcp*

**Static IP:** *netsh interface ip set address "Local Area Connection" static 125.187.7.56 255.0.0.0*

**Set DNS Server:** *netsh interface ip set dns "Local Area Connection" static 192.168.0.200*

Configure Dynamic Host Configuration Protocol (DHCP)

Below is a quick review of DHCP terminology:

<b>scope</b>	A scope defines a single physical subnet on your network to which DHCP services are offered, and is a consecutive range of deployed IP addresses for a network. Scopes give administrators a primary mechanism for the management, distribution and assignment of IP addresses. It also allows configuration parameters to be sent to clients on the network.
<b>superscope</b>	An administrative group of individual scopes that can provide a means to support multiple logical IP subnets on the same physical subnet. Superscopes can only contain a list of child or member scopes that can be activated together.
<b>exclusion range</b>	An exclusion range is a set of IPs that will be excluded from automatic assignment, and are typically reserved for static addressing. Exclusion ranges assure specific addresses within these ranges are not offered by the server to DHCP clients on your network.
<b>address pool</b>	This is the set of addresses that are available for assignment via DHCP.
<b>lease</b>	A lease the amount of time that a DHCP server specifies that a client will maintain a dynamically provided address. Once assigned to a network node, the lease is deemed active. Before the lease expires, the client will attempt to renew the address.
<b>reservation</b>	Reservations are used to ensure that a network node always receives the same IP.
<b>option types</b>	Option types configuration parameters a DHCP server can provide when serving leases to DHCP clients. Some commonly used options default gateways, DNS servers, and WINS servers. Typically, these option types are enabled and configured for each individual scope.

**Figure 11:** DHCP Terminology

Installing and configuring DHCP is accomplished through a set series of steps:

1. Install DHCP by enabling a role on a specific server through server manager. Open server manager, click add roles, and then choose the DHCP Server Role.
2. You will be prompted to specify the Network connection binding by choosing the network on which DHCP services are enabled.
3. Specify the parent domain that the clients are members of as a fully qualified domain name (network.com).
4. You will then enter the DNS server, and can click validate to test the connection.
5. You can optionally enter a WINS server IP Address.
6. To Add or Edit, click on Add Scopes. You need to enter all the required information, and can designate a scope as Wired or Wireless. When complete, you can Activate the Scope.
7. Choose whether or not you want to enable the server for IPv6 stateless mode.
8. Authorize the server within the Active Directory Domain Service. You can use either current credentials, or specify alternate credentials for authorization. Note: You must authorize the server before it can start assigning IP addresses.

## Configure routing

Windows Server 2008 includes many enhancements to Routing and Remote Access:

- **Server Manager** – As with most functionality within 2008, Server Manager gives the IT administrator a simple way to install and configure services. The Routing and Remote Access role is added through the server manager Add Role dialog, and once added, all configuration can be accomplished through this interface.
- **SSTP Tunneling Protocol** – Server 2008 provides a new Virtual Private Networking (VPN) technology called Secure Socket tunneling Protocol (SSTP). This protocol provides features that allows pass-through VPN traffic, when dealing with firewalls and other network security devices that typically block PPTP and P2TP. The technology provides secure access through SSL with HTTPS over port 443.
- **VPN enforcement for Network Access Protection (NAP)** – NAP provides a client health policy enforcement technology to require specific client configurations and requirements. Server 2008 requires clients to be in compliance with software requirements, configuration requirements and update requirements before they can connect to a corporate site via VPN. This provides a powerful security tool to ensure rogue devices cannot enter a secure and protected network.
- **IPv6 Support** – Server 2008 provides the following IPv6 enhancements with regards to cryptographic support:
  - ▶ Protocols-PPPoE, PPPoE over dial-up/Ethernet as well as VPN tunnels, L2TP over IPv6, DHCPv6 Relay Agent.
  - ▶ Stateless filtering, based on the following parameters: Source IPv6 address/prefix, Destination IPv6 address/prefix, Next hop type (IP protocol type), Source Port number (TCP/UDP), Destination Port number (TCP/UDP).
  - ▶ RADIUS over IPv6 transport.

Server 2008 RRAS has quite a few features that have been disabled/removed from previous versions of the service.

- Bandwidth Allocation Protocol (BAP)
- X.25
- Serial Line Protocol (SLIP)
- IP over IEEE 1394
- Asynchronous Transfer Mode (ATM)
- Legacy Novell Protocols – NWLink/IPX/SPX
- NetBIOS
- Services for Mac
- Open Shortest Path First (OSPF) Routing Protocol
- Basic Firewall
- SPAP, MS-CHAP, EAP-MD5-CHAP



Windows provides the Route command to allow administrators to view and set routing information through a command line interface. Below are some summary commands:

**route print -4** : will display the IPv4 Routing Table.

**route print -6** : displays the IPv6 routing table.

**route -p add 192.168.1.0 mask 255.255.255.0** : adds a persistent static route to the routing table.

A persistent route will not be removed when the computer is restarted.

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\sboals>route print -4
=====
Interface List
33 ..... PSIGEN HQ
11 ..00 21 00 e4 0f 81 ..... Broadcom 4322AG 802.11a/b/g/draft-n Wi-Fi Adapter
10 ..00 23 5a a3 f6 b6 ..... Realtek RTL8102E Family PCI-E Fast Ethernet NIC (NDIS 6.0)
1 ..... Software Loopback Interface 1
18 ..00 00 00 00 00 00 e0 isatap.psigen.com
25 ..00 00 00 00 00 00 e0 isatap.calwisp.com
14 ..00 00 00 00 00 00 e0 isatap.psigen.com
15 ..00 00 00 00 00 00 e0 isatap.psigen.com
16 ..00 00 00 00 00 00 e0 isatap.psigen.com
24 ..00 00 00 00 00 00 e0 6T04 Adapter
23 ..00 00 00 00 00 00 e0 isatap.psigen.com
34 ..00 00 00 00 00 00 e0 Microsoft ISA/TAP Adapter #6
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway           Interface         Metric
0.0.0.0                    0.0.0.0          192.168.50.1     192.168.50.103    25
0.0.0.0                    0.0.0.0          192.168.50.1     192.168.50.100    20
70.165.51.51              255.255.255.255 192.168.50.1     192.168.50.103    26
127.0.0.0                  255.0.0.0        On-link          127.0.0.1         306
127.0.0.1                  255.255.255.255 On-link          127.0.0.1         306
127.255.255.255           255.255.255.255 On-link          127.0.0.1         306
192.168.1.0                255.255.255.0   192.168.1.200   192.168.1.202     26
192.168.1.202             255.255.255.255 On-link          192.168.1.202     281
192.168.50.0              255.255.255.0   On-link          192.168.50.103    281
192.168.50.0              255.255.255.0   On-link          192.168.50.100    276
192.168.50.100            255.255.255.255 On-link          192.168.50.103    281
192.168.50.255            255.255.255.255 On-link          192.168.50.103    281
192.168.50.255            255.255.255.255 On-link          192.168.50.100    276
224.0.0.0                 240.0.0.0        On-link          127.0.0.1         306
224.0.0.0                 240.0.0.0        On-link          192.168.50.100    276
224.0.0.0                 240.0.0.0        On-link          192.168.50.103    281
255.255.255.255           255.255.255.255 On-link          127.0.0.1         306
255.255.255.255           255.255.255.255 On-link          192.168.50.100    276
255.255.255.255           255.255.255.255 On-link          192.168.50.103    281
255.255.255.255           255.255.255.255 On-link          192.168.1.202     281
=====
Persistent Routes:
None
C:\Users\sboals>
```

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\sboals>route print -6
=====
Interface List
33 ..... PSIGEN HQ
11 ..00 21 00 e4 0f 81 ..... Broadcom 4322AG 802.11a/b/g/draft-n Wi-Fi Adapter
10 ..00 23 5a a3 f6 b6 ..... Realtek RTL8102E Family PCI-E Fast Ethernet NIC (NDIS 6.0)
1 ..... Software Loopback Interface 1
18 ..00 00 00 00 00 00 e0 isatap.psigen.com
25 ..00 00 00 00 00 00 e0 isatap.calwisp.com
14 ..00 00 00 00 00 00 e0 isatap.psigen.com
15 ..00 00 00 00 00 00 e0 isatap.psigen.com
16 ..00 00 00 00 00 00 e0 isatap.psigen.com
24 ..00 00 00 00 00 00 e0 6T04 Adapter
23 ..00 00 00 00 00 00 e0 isatap.psigen.com
34 ..00 00 00 00 00 00 e0 Microsoft ISA/TAP Adapter #6
=====

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
1 306 ::1/128 On-link
10 276 fe80::64 On-link
11 281 fe80::64 On-link
11 281 fe80::c09:b8cc:7aa9:76e0/128 On-link
10 276 fe80::7d3f:2c3f:5596:19ac/128 On-link
1 306 ff00::8 On-link
10 276 ff00::8 On-link
11 281 ff00::8 On-link
=====
Persistent Routes:
None
C:\Users\sboals>
```

Figure 12: Route Table

Routing Information Protocol (RIP) is a routing protocol provided with RRAS. RIP provides the ability to exchange routing information between configured routers. It is extremely simple to deploy, but has a 15 hop count limit, so it cannot be deployed within large networks. RIP also has long recovery times for down links, and can take several minutes to reconverge routing data in larger deployments. To enable RIP:

1. Under RRAS, expand IPv4, and right-click General, and choose New Routing Protocol.
2. Choose RIP v2, click OK, and it will now appear under IPv4.
3. To configure the interface on which you want to activate the protocol, right-click RIP and click New Interface. You will need to select the subnet where the remote router is connected, and click OK.
4. When your changes are saved, RIP will now automatically exchange information.

Server 2008 has improved its RIP implementation, and it now includes the following features:

- Selection of which RIP version to run on each interface for incoming and outgoing packets.
- Split-horizon, poison-reverse, and triggered-update algorithms that are used to avoid routing loops and speed recovery of the network when topology changes occur.
- Route filters for choosing which networks to announce or accept.
- Peer filters for choosing which router's announcements are accepted.
- Configurable announcement and route aging timers.
- Simple password authentication support.
- The ability to disable subnet summarization.

## Configure IPsec

Windows Server 2008 include the following improvements to Internet Protocol security (IPsec):

- **Integrated firewall and IPsec configuration** – Server 2008 has combined the configuration of the firewall and IPsec. In previous versions, they were two separate entities that had to be configured separately, and it was possible to have conflicting and contradictory settings between the 2 services. The services are now configured through a single snap-in interface, and can also be configured through netsh.
- **Simplified IPsec policy configuration** – typical networks have a need for both secured communications, as well as communications in the “clear” or unencrypted. Unencrypted communications include access to standard network services like DHCP, DNS and domain controllers. Windows now includes parallel communications channel capabilities, and will initiate communications on both secured and non-secured channels. This negotiation behavior allows for simplified rule creation.
- **Client-to-DC IPsec protection** – client-to-domain controller encryption has been difficult and problematic in the past, due to a variety of factors, especially when building new clients that have no domain membership. With Server 2008, you can now deploy IPsec for DC-client communications, and not require encrypted communications, so domain joins can be done via clear channels. Now there is no need to create complex exception rules in IPsec policy for domain traffic.

- **Improved load balancing and clustering server support** – failover times in server 2003 were unacceptable, and it typically took up to 2 minutes to reconnect during a failure. 2008 now takes advantage of new features in IPv6 to provide for rapid failure, through the use of segment retransmission.
- **Improved IPsec authentication** – 2003 had some limitations on how it provided authentication through IKE. The system authenticated the machine, but not the user. 2008 now provides the following improvements:
  - ▶ Health certificates to authenticate IPsec Peers using Network Access Protection.
  - ▶ Second tier authentication requiring user-based or health based authentication methods using Kerberos, NTLM or certificates.
  - ▶ Enhanced mutual authentication through multiple methods.
- **New cryptographic support** – with the advent of additional governmental requirements for stronger cryptography standards, 2008 adds a number of new algorithms for negotiation, encryption, and data integrity.
- **Integration with Network Access Protection** – NAP provides that clients meet certain “health” requirements before being allowed to complete secure connections.
- **Additional configuration options for protected communication** – new settings that provide simplicity in configuration on the following points: specify by application name, port range, adapter specifics, AD user or computer account, ICMP types/codes, and for services.
- **Integrated IPv4 and IPv6 support**
- **Extended events and performance monitor counters**
- **Network Diagnostics Framework support** – provides enhanced troubleshooting and problem resolution framework for connection issues.

To configure IPsec, you need to open the Windows Firewall with Advanced Security on the Local Computer, and click the Customize button on the IPsec Settings tab. You will then be able to customize the IPsec settings, through the presented dialog box:

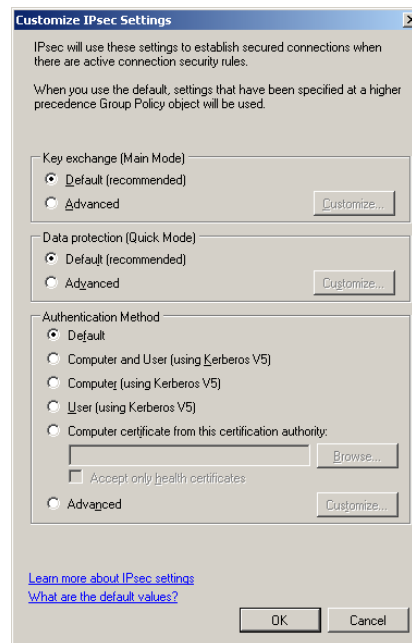


Figure 13: IPsec Settings

The three sections on this tab can be summarized as:

- **Key Exchange (Main Mode).** You can use this mode to enable secure communication. Two computers must be able to access the same shared key locally. Click the **Customize** button to configure security methods/settings, key exchange algorithms, and security key lifetimes.

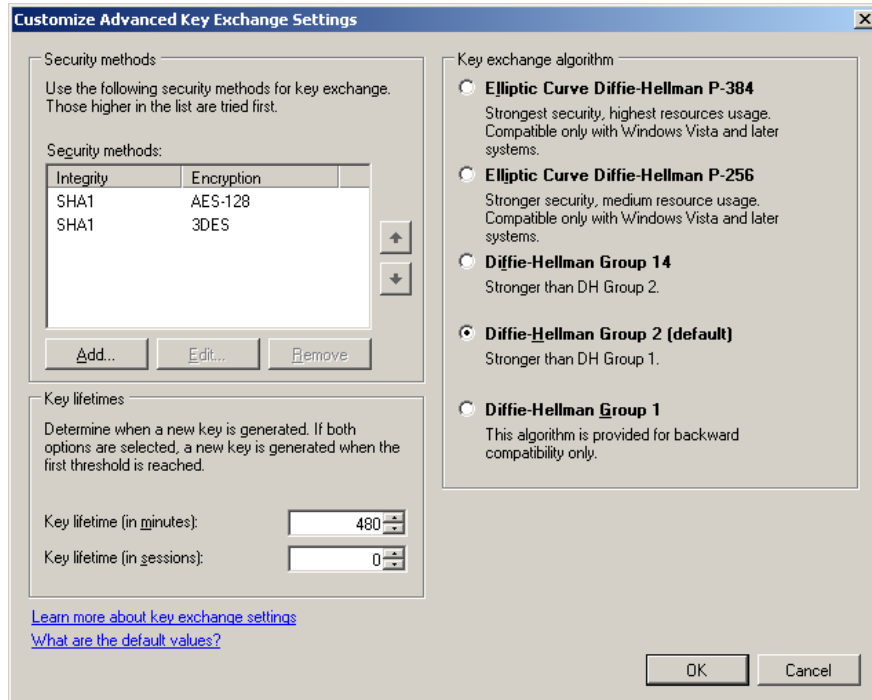


Figure 14: Customizing Advanced Key Exchange Settings

The primary use of these settings are to protect the IPsec negotiation process that will in turn determine the protection method used for the rest of the data communications over the established connection.

- **Data Protection (Quick Mode).** This mode defines the protocols and algorithms used to provide data integrity and encryption for an established secure connection. The data integrity process ensures that data is not modified or altered in any way during transit. Data encryption uses cryptographic algorithms to protect the communicated information. Windows Firewall with Advanced Security uses Encapsulating Security Payload (ESP) or Authentication Header (AH) to provide data protection, and ESP for data encryption.

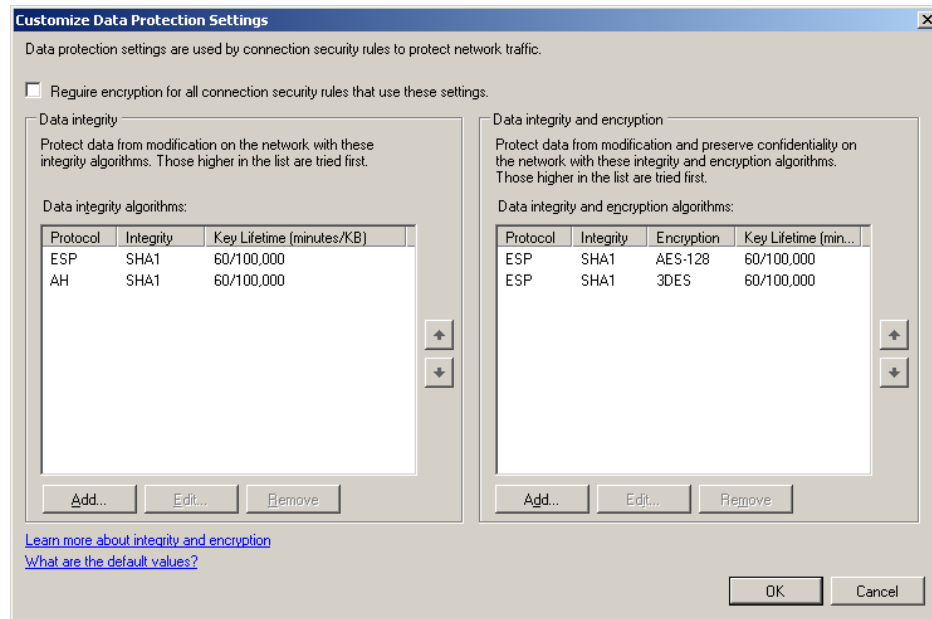


Figure 15: Date Protection Settings

- **Authentication Method.** This setting lets you establish the default authentication method for secure connections on the local computer. Note: group policy will override this local setting if a different method is specified by a rule or by Group Policy settings. The default authentication method is Kerberos version 5. You can also restrict connections to only those entities that have a signed certificate from a specified certification authority (CA). Other options include:
  - ▶ **Public key certificates** – used with partners that may have a PKI configuration.
  - ▶ **Preshared key** – used with Mac, Windows 98 or unix based client networks.

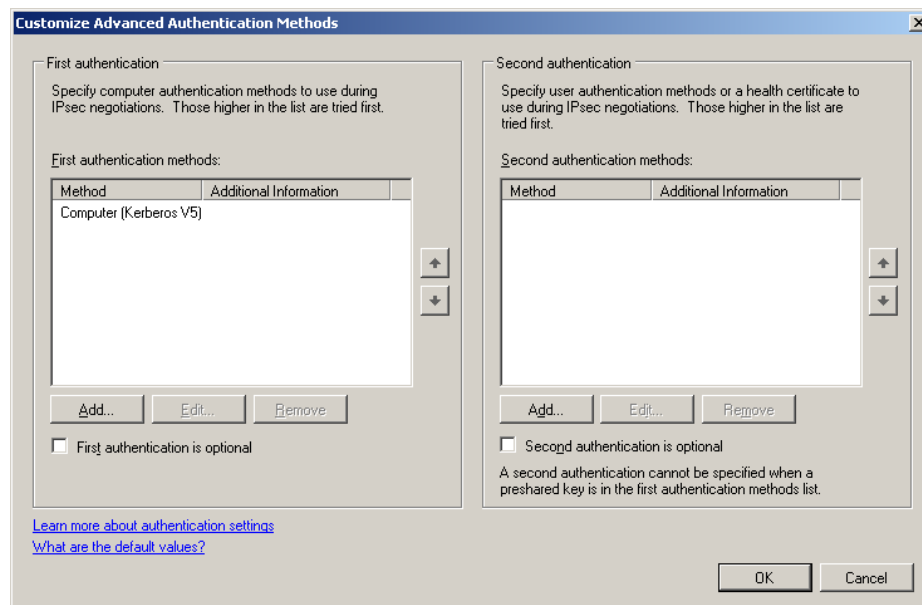


Figure 16: Advanced Authentication Methods

IPSec Policies are used to create set templates for security services configuration. The policies are created with the IP Security Policies Snap-in, and once created can be applied to the domain, site, organizational unit and local level. To create a new policy, some general steps can be applied:

1. Create IP Filters that represent the networks, computers and conditions within your IT infrastructure.
2. Once the filters are created, you can then create filter actions that are rule sets on how connections are established, authenticated, encrypted and how data integrity is applied.
3. Once the filters and filter actions are created, then you can create security policies that match your overall requirements.
4. Deploy Permit and Block policies, and monitor your environment to alleviate any issues that may occur.
5. The policies are then deployed with the Negotiate Security filter action. If you set the option to fall back to clear text, you can test the policy in your environment with minimal impact.
6. After you have fine tuned the policy, you can remove the clear text fallback option and go fully secure.
7. Always monitor and test the deployed policy.

## Monitoring and Managing a Network Infrastructure

### Configure Windows Software Update Services (WSUS) server settings

Windows Server Update Service (WSUS) provides the ability to manage and distribute the latest Microsoft updates across their network to participating clients. The latest version, WSUS 3.0 SP2 provides new windows server and client support with integration to:

- Windows Server 2008 R2
- Support for Windows 7 clients
- Support for BranchCache on Server 2008

The major feature enhancements in the latest version include:

- **Auto-approval rules** – provides the capability to specify the approval deadline for specific computer groups and or individual computers.
- **Easy upgrade** – an in place upgrade is now available, and you can upgrade existing WSUS implementations and keep all your approvals and settings.
- **Update Files and Languages** – provides specific language designation and warning dialogs for downstream servers.
- **Reports** – You can now run reports from the console or use the API.

- **Windows Update Agent (WUA) Improvements** – the new WUA client has been vastly improved, with enhancements to performance, user experience and bug/functionality enhancements based on feedback.
  - ▶ Faster client scan time
  - ▶ Scoped scan options, instead of full scans, provide rapid scan capabilities
  - ▶ Display improvements

Below are the system requirements for installing WSUS 3.0 SP2:

- Windows Server 2008 R2
- Windows Server 2008 SP1 or later
- Windows Server 2003 SP1 or later
- Windows Server SBS 2003/2008
  - ▶ Remove restrictions for an IIS IP or Domain names.
  - ▶ You must configure the proxy server credentials in the form of Domain\user to ensure clients can connect.
  - ▶ If you added any subnets without using the SBS Wizard, you must manually configure the directory security setting in IIS on both the Default and SelfUpdate web roots.
- IIS 6 or later
- MS .Net 2.0+
- One of the following databases:
  - ▶ MS SQL 2008 Express, Standard or Enterprise
  - ▶ SQL Server 2005 SP2
  - ▶ Windows Internal Database
- MMC 3.0
- Microsoft Report Viewer 2008
- Hardware
  - ▶ NTFS
  - ▶ Minimum 1 GB of free space on system partition
  - ▶ Minimum 2 GB of free space on the volume on which DB files will be stored
  - ▶ Minimum 20GB for content storage Terminal Services cannot be running on the computer that is front end for SQL Remote install

The following is a high level overview of the installation steps to get going with WSUS on Windows Server 2008:

1. Open server manager and add the IIS role to your server:

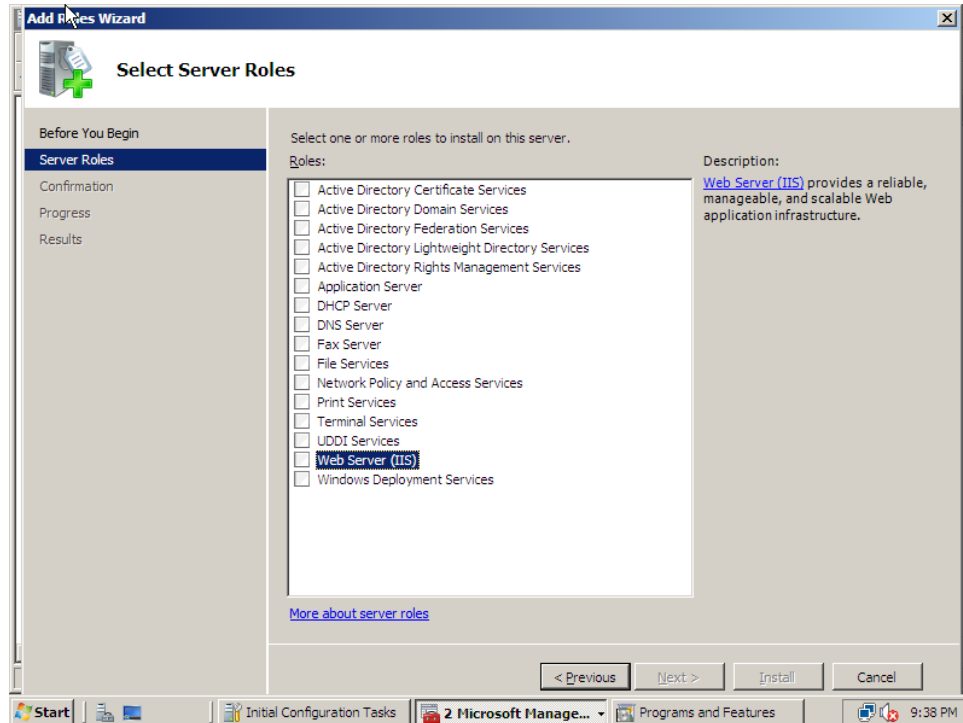


Figure 17: Select Server Roles

2. When prompted, add the required features:

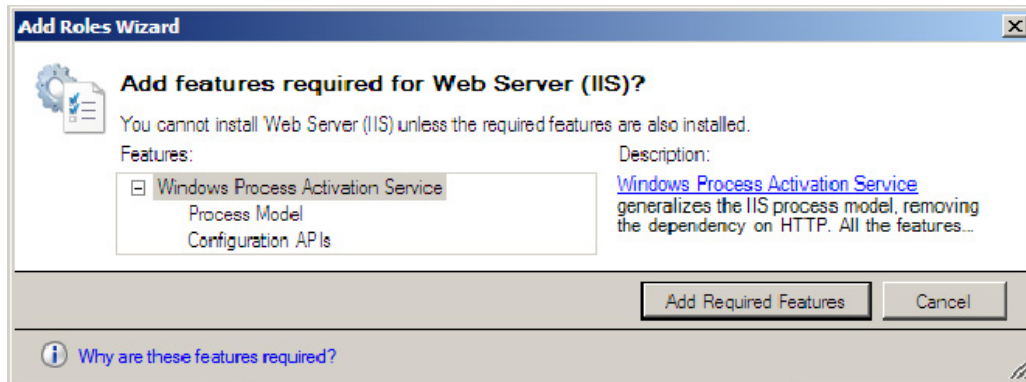


Figure 18: Add Rules Wizard

3. You will need to add a few role services:
  - a. ASP.NET.
  - b. Windows Authentication.
  - c. IIS 6 Metabase Compatibility.
  - d. Insure that HTTP Static content is checked as well.



4. Once you have selected all the Service Role, install IIS.
5. Next, you will need to download Report Viewer 2005, and install the application, along with SP1.
6. Once this is completed, you can now proceed with Installing WSUS SP1.
7. On the Select Update Stores page, ensure you check Store Update Locally, and enter a directory where you will store the updates for client download. If you do not check this box, updates will be downloaded from Microsoft update, and performance will be much slower.
8. You will next be prompted to choose your database options. Note: Production systems should always use SQL.
9. You will now be able to choose to use the default IIS site, or create a site specifically for the update service.
10. On the Upstream Server page you can choose to receive your updates from Windows Update, or specify an upstream server within your organization that will pass you updates. This is a great feature for branch offices, as they can receive their updates from a central corporate server.
11. Finally, you can choose which Windows products you would like to provide update services for.

WSUS provides an update mechanism and management infrastructure consisting of the following:

- **Microsoft Update** - the Microsoft Web site that distributes updates for specific Microsoft products. This is the top level of the hierarchy, controlled by MS.
- **Windows Server Update Services (WSUS) server** - the component that is installed on a server running Windows Server 2008 within the organization. WSUS provides the ability to administrators to manage, distribute and choose updates through the administrative console, which can manage all WSUS servers in any domain with which it has a trust relationship. A WSUS server can obtain updates either from Microsoft Update or from an upstream WSUS server, but at least one WSUS server in the network must connect to Microsoft Update to get available updates, and this server is the top level of the hierarchy. WSUS can be deployed in several ways, and IT can decide how many WSUS servers can connect directly to Microsoft Update, based on available bandwidth, network configuration, and security provisions. These top level servers can then distribute updates to other downstream servers.
- **Automatic Updates** - this is the client computer component built into the Windows operating system. Automatic Updates provides update services to server and client computers, and allow them to receive updates either from a WSUS server or Microsoft Update.

WSUS allows for hierarchical deployment to ensure uniform distribution of updates. This hierarchy allows for servers to download updates from upstream servers, with the server at the very peak of the hierarchy controlling distributed updates. When building this infrastructure, there are two administrative modes:

- **Replica Mode** – when a server is placed in this mode, all computer group settings and update approvals are inherited from its upstream server. This is the best setting for a branch organization structure, as it allows for a central server to control updates.
- **Autonomous mode** – In autonomous mode, the administrator always controls all the settings and approvals. This is the typical mode for the central or top-level server.

Software updates are what WSUS distributes, and Software updates consist of two parts:

- **Update files** - the actual install files that are downloaded and installed on client computers.
- **Update metadata** - the information needed to execute the software installation, which includes:
  - **Update properties** - title, description, KB article, Microsoft Security Response Center number.
  - **Applicability rules** - these are used to determine whether an update needs to be applied to the client.
  - **Installation information** - command-line options for application install.

The update components can be downloaded separately to the individual client computers. For example, if you select not to store updates on the local machine, only update metadata (and any applicable Microsoft Software License Terms) will be downloaded to the WSUS server and the clients will get their update downloads directly from Microsoft Update. If you are storing updates locally on the WSUS server, you can download everything at the time of synchronization, or download only the metadata, leaving the downloaded update files to be sent after you have approved the update.

WSUS downloads update during the synchronization process, and the initial download can take quite a while to synchronize. The WSUS server will download only new updates after the first sync from the update source, and also synchronize the metadata for expiration and updates as well. The Options page is where synchronization is configured, and you can specify:

- Where your server gets updates: upstream server of Windows Update
- Designate automatic updates for synchronization
- Connection settings
- Sync Schedule

WSUS downloads updates based on the designated products/product families and classifications. Under the Options Tab, you can specify Products and Classifications:

- **Products** – grouped by product family. Selecting the parent level will select all the child nodes in the product family set. You can select individual products by choosing the child node only.
- **Classifications** – are specific types of updates you intend to apply. For example critical updates.

## Capture performance data

Windows 2008 provides an MMC snap-in called Windows Reliability and Performance Monitor which provides an all-in-one interface for monitoring servers and troubleshooting. The snap-in combines all the functionality of previous standalone tools: Server Performance Advisor, Performance Logs and Alerts and System monitor.

The interface is very well laid out, and its primary purpose is to correlate stability to key events. For instance you can track stability after installing a new application or patch. The interface can be opened through the MMC by adding the Reliability and Performance Monitor Snap In. You can also access the interface through the Server Manager Diagnostics.

Server 2008 provides several new key features for monitoring performance and reliability:

- **Templates and Wizards for log creation** – 2008 provides an easy wizard interface for adding counters to log files and setting schedules.
- **Data Collector Sets** – you can now create specific sets of collected data as reusable templates.
- **Resource view** – this interface resembles that of task manager, and gives you a real time view of processor, memory, disk and network usage.
- **Reliability Monitor** – provides the ability to automatically graph system stability and reliability over time through a calculated index.
- **Unified configuration** - for all scheduling and collection activities.
- **Diagnosis Reports** – a set of easily configured reports for diagnosing server issues.

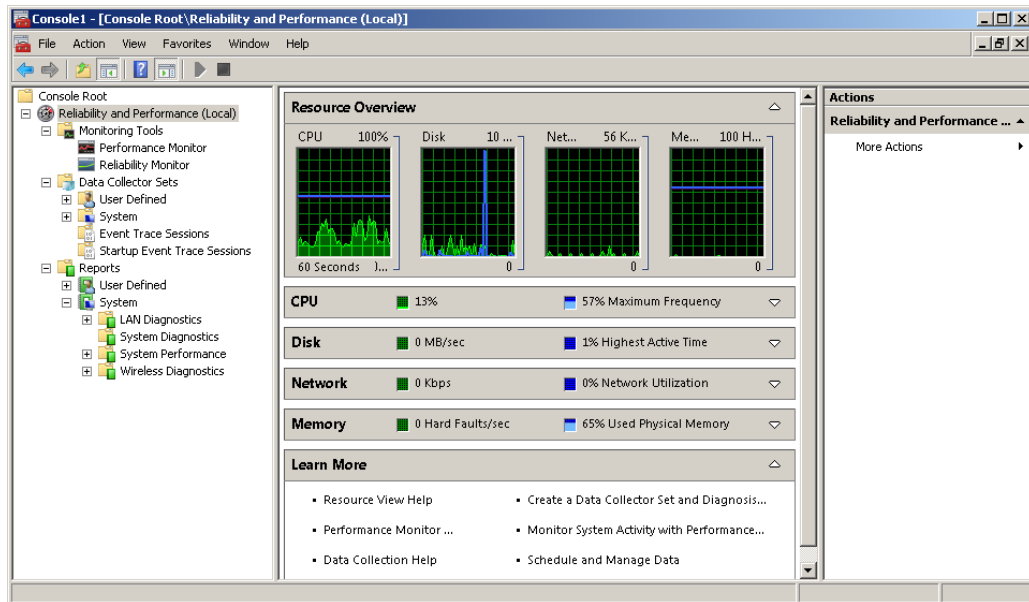


Figure 19: Resource Overview

## Performance Monitor

Those who have been around windows for a while will recognize their old friend, with some new graphics. Just as in the old version, just simply click the “+” to add a counter. Use CTRL+H to highlight a counter, and right click the counter to view a variety of options shown below:

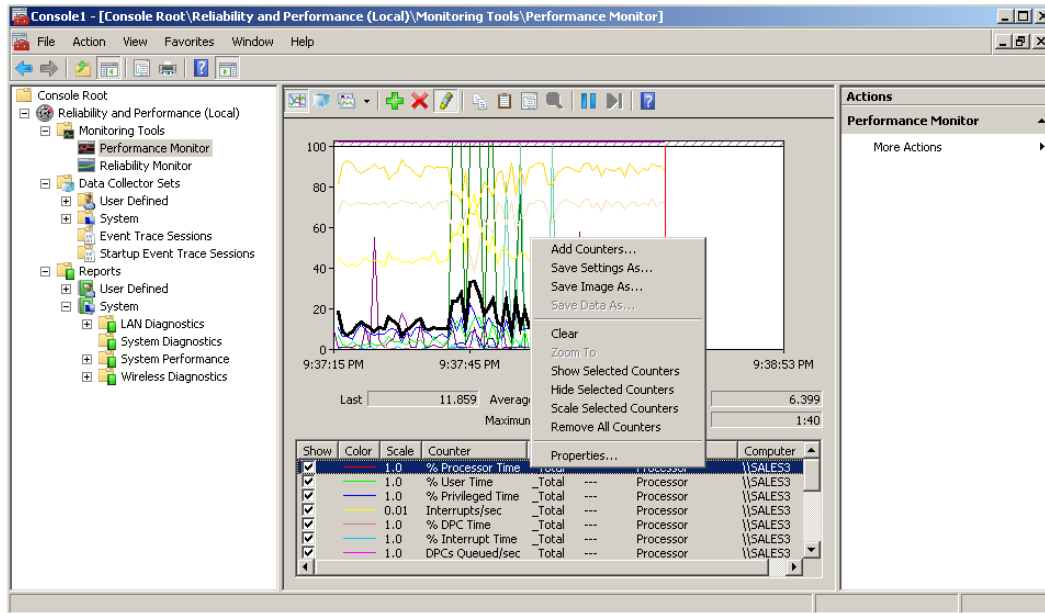


Figure 20: Properties

Right-clicking and selecting properties will give you a five-tabbed property window, with the following options:

- **General** – provides the ability to tailor the graph and sample interval.
- **Source** - provides the ability to view real-time data, specify a log file for graphing, and even set a database to pull information from. You can also tune the time interval.
- **Data** - allows you to add and remove counters, set colors, style and scale.
- **Graph** – provides several graphing options and axis label options.
- **Appearance** – controls font, background and colors.

Performance monitor can be an invaluable tool in collecting data and troubleshooting. As in previous versions of the OS, the application provides numerous counters on system resources that can be monitored and tracked:

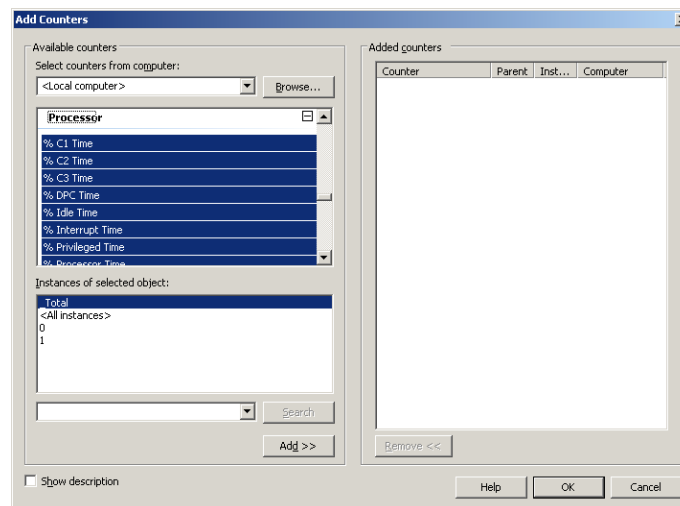


Figure 21: Add Counters

To configure a counter, click the plus button, expand the counter section, and highlight the counters to add.

There are several counters that can be used to monitor system performance problems. Below is a guide for specific issues:

- Storage related monitoring - these can be used to isolate disk/storage related I/O problems on servers with heavy workloads.
  - Average Disk Queue/ Current Disk Queue length – this is one of the most important counters, and will show the number of queued requests for the I/O subsystem, and can be indicative of issues when quite large.
  - Disk Reads/Writes/ Transfers per second – can be used with the queue length above to show actual activity versus a bulding queue.
  - Active Directory Specific Issues – on domain controllers, you can use the following counters to examine performance and resolve issues: To examin the amount of memory being used by the lsass.exe, setup a specific counter to track the service. If high physical memory, then you can use:
    - Database Cache % Hit and Database Cache Size – these counters can indicate whether additional memory can improve AD issues.
  - If lsass.exe is using high CPU, used Directory Services\ATQ Outstanding Queued Requests to see how many requests are waiting. This is typically indicative of a slow disk subsystem.

## Reliability Monitor

The reliability monitor gives you a great snapshot of your system stability:

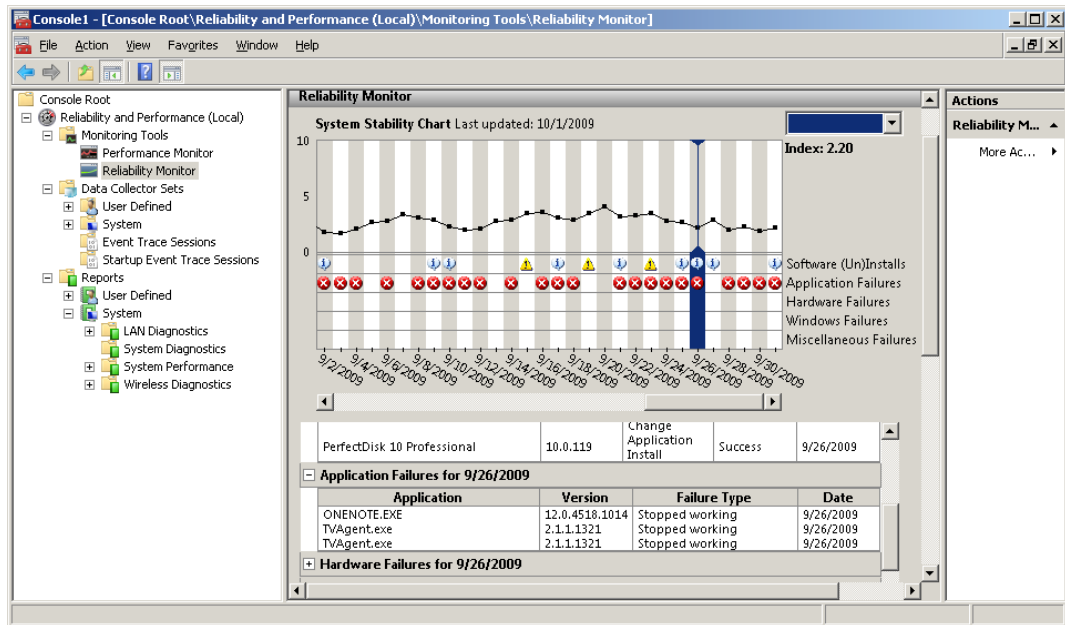


Figure 22: Reliability Monitor

The interface shows a multi-faceted graph that will include an overall stability rating on a scale of 0-10, and lists the following items with dates, time and details:

- Software installs/uninstalls
- Application Failures
- Hardware Failures
- Windows Failures
- Misc Failures

One of the key features is the **System Stability index**. This calculation is based on data that is collected over the lifetime of the system, and each date within the System Stability Chart includes a graph point showing that day's System Stability Index rating. The System Stability Index has a scale, with a number from 1 (least stable) to 10 (most stable). The index is a weighted measurement calculated from the number of failures seen over a rolling historical period. Reliability Events (as listed above) within the System Stability Report describe the specific failures. Below are more details:

- More recent failures are weighted more heavily in the overall calculation than past failures. This allows an improvement over time to be shown in an ascending System Stability Index once a reliability issue has been resolved.
- Power off or sleep state periods are not used when calculating the System Stability Index.
- If there is not enough data to calculate a steady System Stability Index, it will be reflected in the graph, as the graphed line will be dotted. A solid line indicates enough data has been recorded to generate a steady System Stability Index.
- An Information icon will appear on the graph for each day on which the system time was adjusted.

### Data Collector Sets

Microsoft has established a building block approach to performance monitoring through the use of Data Collector Sets. They allow the organization of multiple collection points, housed within a single container that can be reused. The sets can be used to:

- Review or log performance
- View stats in performance monitor
- Configured to generate alerts

To create a Data Collector Set:

1. Go to Performance Monitor and add counters to create a custom view.
2. Right-click the Performance Monitor, select New, and click Data Collector Set. The Create New Data Collector Set Wizard starts. The Data Collector Set created will contain all of the data collectors selected in the current Performance Monitor view.
3. Enter a name for your set.
4. By default, the Root Directory will contain data collected by the Data Collector Set. You can change this to store the information in a custom location.
5. After clicking Next, you can configure the user to run the Data Collector Set. Click the Change button to enter the user name and password for a different user than the default listed.
6. Click Finish.

## Monitor event logs

Server 2008 provides access to the event viewer interface wither through the Event Viewer snap-in, or under diagnostics within Server manager. 2008 has provided several enhancements to event logging, including:

- Clarification and enhancements to message text to provide more informative messages.
- Additional logs specific to server functions and services to isolate and track issues.
- Usage of a Windows Internal Database or third party database as well.
- Enhanced event forwarding capabilities.

## Application and Service Logs

Application and Service logs are provided within Server 2008 as a new location to store information about individual applications and/or components. They are an excellent troubleshooting tool when looking at specific application issues, or problems between applications. There are four types of sub logs:

- **Admin** – these logs provide guidance to administrators on problems where there is a defined action that can fix the issue.
- **Operational** – these event types are used to diagnose and provide details to analyze a problem. They typically log operational events within windows, such as when a device is added to a computer.
- **Analytic** – These events describe program operation and can help identify problems and troubleshooting steps.
- **Debug** – This log is used by developers to help isolate and identify issues within code and applications.

To find out what type of log you are viewing, you can right-click and view the properties. The log type is shown in the header. Note: In 2008 you can attach tasks to these logs, and have the ability to start a program, send an email or display a message when a log entry is created.

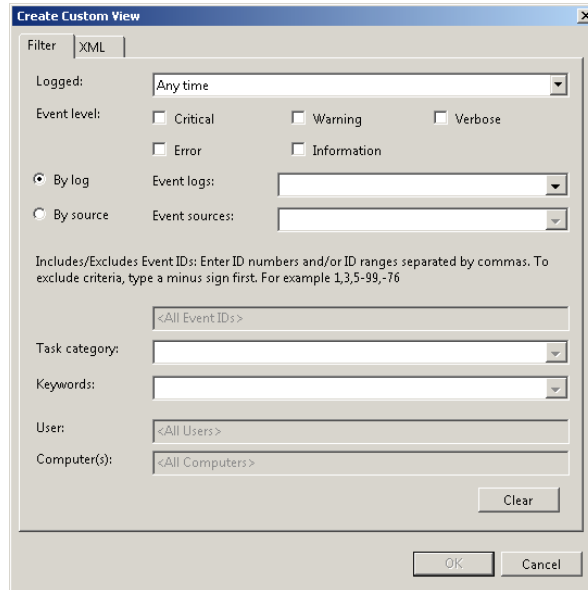
Note: Analytic and Debug logs are need to be enabled manually due to their heavy loggin load on a system and should be used with discretion as they can really bog down a system that has high usage.

## Custom Views

Event logs can contain a very large amount of loggin information and it is sometimes impossible to go through each event one by one to isolate the information you are seeking. There are two ways to present only the entries you seek: filters and views. Filters are not persistent, and mut be recreated. Views can be created, and then applied to multiple logs, and saved. Within the Event Viewer, Windows Server 2008 provies the ability to create views across multiple logs.

Creating a custom view is accomplished through the following steps:

1. Choose the Create Custom View selection in the Action menu within the event viewer.
2. The Create Custom View dialog will open, and you can select the event level, log, sources, keywords, etc, as shown below:



**Figure 23:** Create Custom View

3. Once you select the By Log or By Source selection, you will get additional details in the Task Category and keywords specific to that log. Note: Windows will automatically build the XML query for you that can be altered, saved, imported or exported.

Importing and exporting custom views can be accomplished through the use of the XML that is created when configuring a view. Once you have created a view, you can export it by right-clicking and choosing the export option. To import, you can right-click the Custom Views node in the Event Viewer and choose import. Note: You can also save a filter you have created by right-clicking and choosing to Save Filter as a Custom View.

## Event Forwarding and Subscriptions

Server 2008 provides the ability to centrally collect and manage events throughout the organization through the use of Event Forwarding and Subscriptions. This allows a single computer, or collector, to receive log entries over HTTP or HTTPS, providing a standardized transfer method for communications. Event forwarding requires the configuration of both the collector computer and the source computer.

Full list of requirements for enabling event forwarding:

- HTTP and HTTPS ports allowed (port 80 and 443)
- Windows Remote Management Service Enabled
- Windows Event Collector Service enabled
- Source computer configured
- Collector Computer configured



The collector computer needs to be running one of the following operating systems:

- Windows Server 2008
- Windows Server 2003 R2
- Windows Vista

The source computer must be running:

- Windows XP SP2
- Windows Vista
- Windows Server 2008
- Windows Server 2003 R2

There are two types of subscription configurations that can be enabled:

- Source-initiated – In this type of setup, the source computer will send a message to the collector whenever an event is generated. This type of setup is best for an environment that has a large number of client computers that can be configured through Group Policy. This is also known as a push configuration.
- Collector Initiated – in this setup, the collector will poll the computers on the network, and retrieve any log entries. This is appropriate for small networks.

Below are the steps to configuring a collector-initiated setup:

1. On each of the source computers, open an elevated privilege command prompt, and enter:  
*winrm qc*

```
Administrator: C:\Windows\system32\cmd.exe - winrm quickconfig
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\shoals>winrm quickconfig
WinRM is not set up to allow remote access to this machine for management.
The following changes must be made:

Set the WinRM service type to delayed auto start.
Start the WinRM service.
Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this
machine.
Enable the WinRM firewall exception.

Make these changes [y/n]?
```

**Figure 24:** Elevate Privilege Command

Enter "Y" to start the WinRM service and auto-configure the firewall.

2. You will now have to add the computer account of the collector to the local Administrators Group, or Event Log Readers Group. This can be done either through Local Users and Groups.
3. On the collector computer, open a command prompt and enter: *wecutil qc*. This will enable the Windows Event Collector Service.
4. Now you must configure subscriptions, and define the events you will collect on the collector.

Below are the steps to Configure a source-initiated subscription:

- On the collector computer, you must enter the following commands from an elevated privilege command prompt:
  - Winrm qc -q
  - Winrm qc /q
  - Wecutil cs configuration.xml
- Use gpedit.msc to configure the server address, under Computer Configuration/Administrative Templates/Windows Components/Event Forwarding. Right click and choose properties, enable. Click show to add.

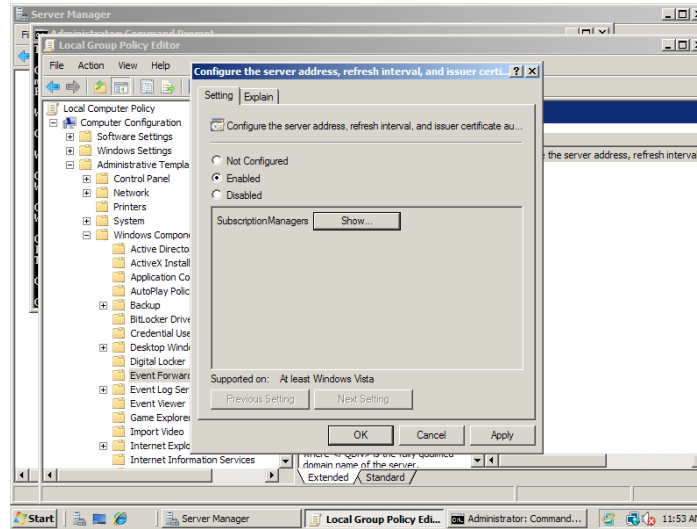


Figure 25: Configure Server Address

- Do a gpupdate /force.

To create an Event Subscription:

- Open the Event Viewer, and right-click the Subscriptions node. Choose Create Subscription.
- The Subscription properties window will open, and there are several options. Enter the name of the Subscription, and a description. You will then need to select the type of subscription you will be creating: Collector-initiated or Source-initiated.

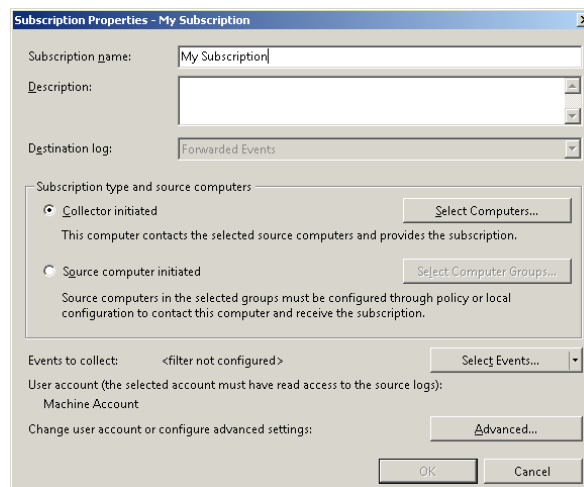
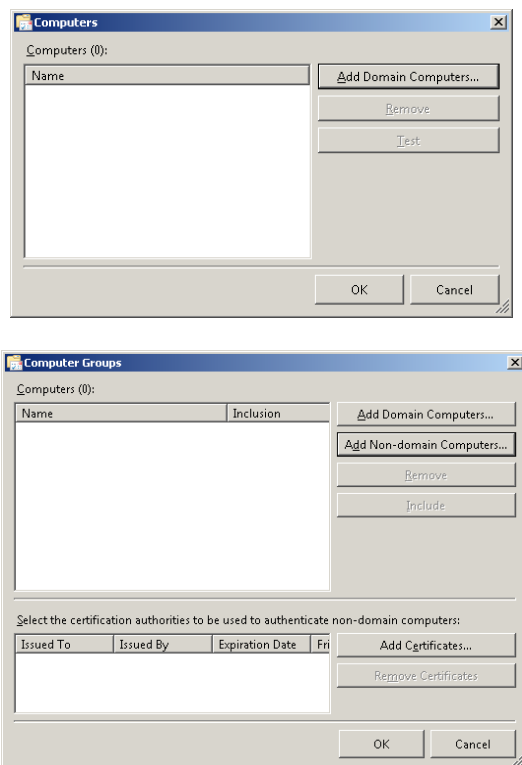


Figure 26: My Subscription

3. If you choose Collector-initiated, simply pick the domain computers from which you want to gather events.
4. The Source-initiated interface is slightly different and gives you the ability to configure both Domain and non-Domain computers. Non-Domain hosts are specified by their DNS name, and you can use wildcards.



**Figure 27:** Computer Groups

5. Once you have specified the above, you can then enter information about the types of events you would like to collect through the Query Filter interface.
6. In the Advanced Subscription settings, you can specify the account for gathering logs, as well as Event Delivery Optimization.

## DNS Logging

The DNS MMC snap-in now includes a Global Logs node that provides a customized log view for DNS events only. The logged events can be configured through the DNS server properties, and provides both generic logging configuration, as well as a built-in Debug Logging tab as shown below:

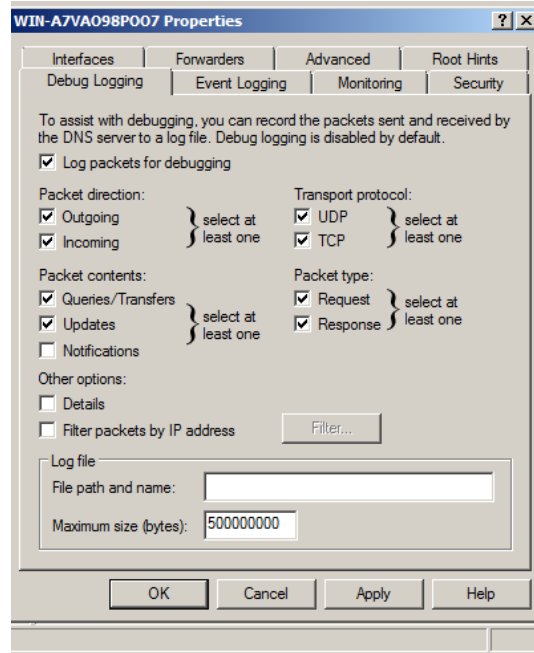


Figure 28: DNS Logging

**Note:** setting DNS debug logging on a heavily used production system will adversely effect performance, and care should be taken to isolate the specific traffic direction and contents required to troubleshoot (as shown above). This can be very handy in troubleshooting name resolution issues with complex DNS infrastructures.

## Gather network data Microsoft Baseline Security Analyzer

The Microsoft Baseline Security Analyzer (MSBA) is a simple, easy to use tool that can gather security state info about your information based on Microsoft security recommendations, and then specify what needs to be accomplished to bring it up to speed. The MSBA is a required tool in today's networks, and security scanning and analysis should be performed on a periodic basis, and whenever infrastructure changes are made, and/or new software is installed.

The MBSA provides the following:

- **Administrative Vulnerability Check** – examines accounts, file shares, formatting, and overall administrative configuration for any vulnerabilities or possible improvements.
- **Security Updates** – gathers information about patches and makes recommended addition suggestions.
- **Password Checking** – will look for weak passwords on target systems.
- **SQL Configuration** – this will examine the configuration of SQL and associated accounts.
- **IIS Configuration** – examines this web service and any security holes.

## Requirements for running MBSA:

- Administrative privileges on the scanning and target computers.
- Scanning computer must have the Workstation Service enabled.
- Scanning computer must have the Client for Microsoft Networks enabled.
- Windows Update Agent 3.0.
- For scanning IIS, IIS source files must be installed.

## Target computer requirements:

- Remote registry service enabled.
- File and Printer Sharing service.
- DCOM.
- Windows Update Agent 3.

Note: The service uses ports 135, 139 and 445 to accomplish all scanning activities and firewalls must have exceptions to allow these ports.

The MBSA can be use through the GUI, or through the command line tool, mbsa.exe. To use the GUI:

1. Go to Start/All Programs and Open the MBSA.
2. You can choose to scan a single computer, or a group of computers.

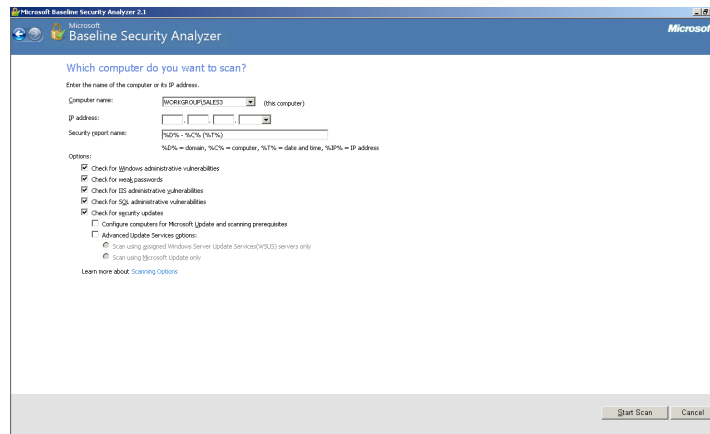


Figure 29: GUI

3. Once selected, you can enter the Computer Name or Address, or the domain name or IP Range for a group.
4. Choose your options, and scan for: admin vulnerabilities, weak passwords, IIS and SQL vulnerabilities, and security update status.
5. The scan will initiate once Start Scan is selected, and the computer (s) will be analyzed and results presented and/or saved.

## Simple Network Management Protocol (SNMP)

SNMP is a network protocol that allows both the polling of devices for status and information and the ability to send “traps” or alerts over the network. Each managed system consists of three separate components: Managed Device, Agent Software and a Network Management System. You must have all of these to take advantage of SNMP and all that it can deliver from a network monitoring standpoint.

There are several Network Management Systems on the market, and the Microsoft products that can centrally manage and gather SNMP information are: System Center Essentials 2007 or System Center Operations Manager 2007. Server 2008 does not include these by default.

On server 2008, SNMP is installed through the Server Manager, by adding features – SNMP Services. Once installed you can configure the service through the registry, group policy, or through the SNMP service Properties. Some import configuration attributes are:

- Community Name – this defines a set of managers and agents and is similar in some ways to a password. You need to know the community to participate.
- Managers – you need to give certain the computers the ability to collect data.
- Trap locations – SNMP traps provide the ability to send error/info messages over the network to a trap collector.

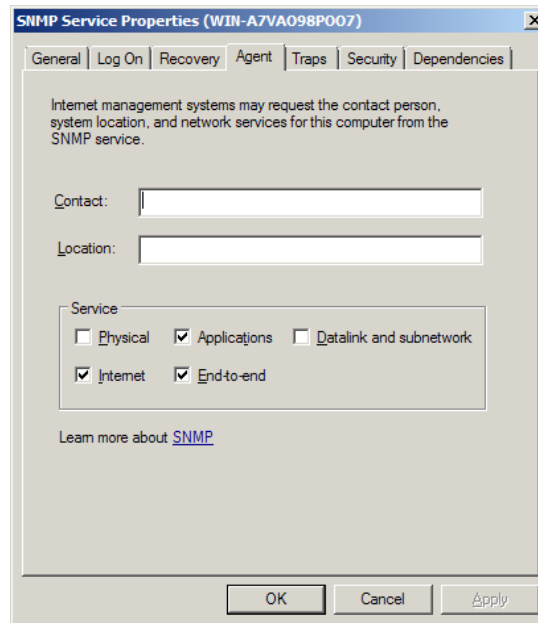


Figure 30: SNMP Service Properties

## Microsoft Network Monitor

Network Monitor is a packet level utility that gives you a looking glass into the network traffic between devices on a network. The application will provide statistics, and allow you to analyze network level issues and traffic problems that can wreak havoc. The Network Monitor displays the following information:

- Frame Number
- Process Name
- Source Address of the sending device
- Destination Address of the receiving device
- Protocols used within the transmission
- Data level information about the transmission

The network monitor will capture all information on a given network interface until the capture process is stopped. Once the capture has been stopped, you can then filter the results to isolate the traffic you intend to examine. In order to use you must have a network interface card that allows promiscuous mode, or the mode that will capture all traffic on the wire. In order to capture traffic on modern switched networks, you may need to enable SPAN/RSPAN on the specific ports to monitor remote ports or enable broadcast traffic to be captured.

Once data has been captured, you can create an alias list to identify addresses to display within the interface. A custom alias list can be created through the following steps:

- From the Display Window, choose the aliases tab.
- Enter the alias name for the entered address to apply custom aliases.

Network captures can be saved, and are designated by a .cap suffix. They can then be reloaded into the viewer to be analyzed at a later time, or compared.

The latest version of Network Monitor includes prebuilt filter sets to provide an easy way to analyze traffic, and also will display application executable names within the left hand window to provide easy filtering. Custom filters can be applied to either the capture process or the viewer through the Display/Capture tabs.

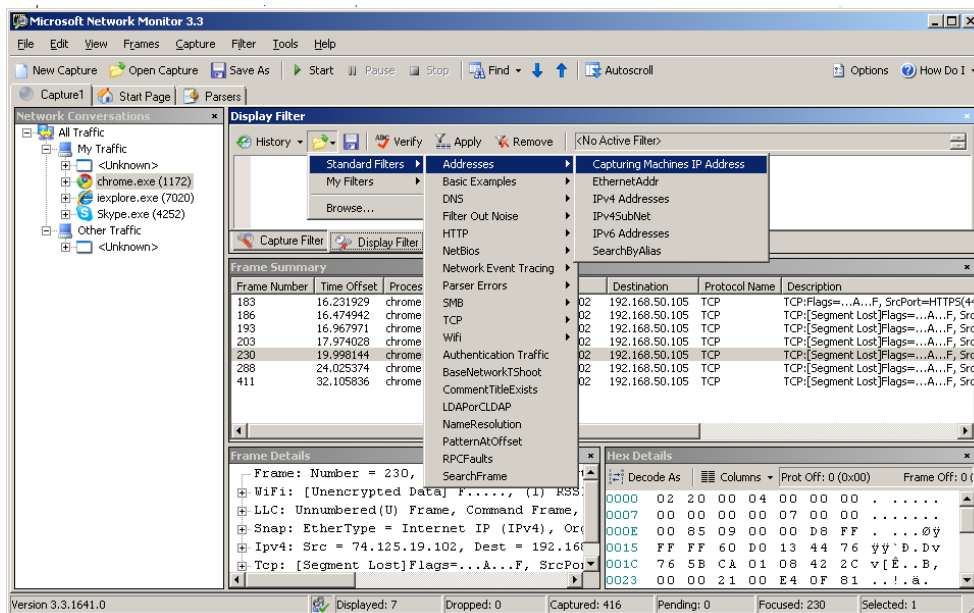


Figure 31: Network Monitor

## Windows Server 2008 R2 Network Monitoring and Management

In Windows Server 2008, several changes were made to the performance and network monitoring solutions within the server. Windows Server 2008 R2 includes the following additional changes to network and system monitoring and management:

- The separation of the **Performance Monitor** and the **Reliability Monitor** is a significant change. The Performance Monitor is now a separate console including support for live performance data evaluations, collection of a data collector set (DCS), and viewing of performance logs and DCS reports. The Reliability Monitor, as a separate tool, is still used to track software and device driver installations and removals on the system. It also tracks historical crashes or system, problems.
- The **Resource Monitor** has been enhanced since its introduction in Windows Vista and Server 2008. In Windows 7 and Server 2008 R2, it offers a process analysis feature that allows you to inspect the wait chain for a non-responding application. The wait chain is simply the list of dependencies upon which the stalled process is waiting. The Resource Monitor also offers an overall facelift making it easier to locate the information you need to analyze or troubleshoot process and performance problems.
- **DirectAccess** is a new feature allowing remote users to connect to the organization's network across the Internet without requiring that they start a virtual private network (VPN) connection. Only Windows 7 clients and Windows Server 2008 R2 servers support the DirectAccess feature. To use DirectAccess, an organization must have a public key infrastructure (PKI) in place as certificates are used for IP Security (IPSec) peer authentication between the clients and servers. Additionally, DirectAccess requires that IPv6 be enabled and configured on both the clients and the servers.
- An additional new feature for remote users is **VPN Reconnect**. With VPN reconnect, Windows 7 clients or Windows Server 2008 R2 clients will automatically reconnect to a VPN server if the connection is temporarily lost. The reconnection can take several seconds, but the process is transparent to the user because any active network transmissions are cached at the VPN server, which must be running Windows Server 2008 R2. VPN Reconnect is only supported with the use of the IPSec tunnel-mode with IKEv2.
- The **BranchCache** feature is also new to Windows 7 and Windows Server 2008 R2. It allows documents to be cached from a remote network onto the local network using either the local Windows 7 clients or a local Windows Server 2008 R2 as the cache storage location. With a distributed cache configuration, the Windows 7 clients simply cache and remote documents on their local systems. When other Windows 7 clients seek the same document, they can use the locally cached copy if the remote document is unchanged. The state of the remote document is quickly verified using hashing algorithms. With a hosted cache configuration, a local Windows Server 2008 R2 server acts as the cache server for all the local clients. BranchCache can be used to cache data transferred using HTTP, HTTPS or Server Message Block (SMB), which means it can cache data stored in remote Windows shares or web servers.



# Deploying Servers

## Deploy images by using Windows Deployment Services

Windows Deployment Services is the enhanced and redesigned version of Microsoft's Remote Installation Services. This service provides the ability to remotely deploy Windows, and has great enhancements when deploying Vista and Windows 7.

Below are the new features provided by WDS when used on Windows Server 2008 R2?

- Operating systems that can be deployed:
  - Windows XP
  - Windows 7
  - Windows Vista SP1
  - Windows Server 2003
  - Windows Server 2008
  - Windows Server 2008 R2
- Image types
  - .wim
  - .vhd images supported and managed through command line
- Windows PE boot environment
- Administration accomplished through MMC or WDSUTIL
- Multicasting support
  - Supported for install images
  - Support for computers with EFI
  - Auto-disconnect for slow connections, and multi-stream support
  - IPv6 support
- Driver support
  - Driver package deployment on Vista SP1, Windows 7 and Server 2008
  - Ability to add drivers to images (Server 2008 R2 and Windows 7)
- Extensibility through PXE support and multicast transmissions
- Extensible Firmware Interface (EFI)
  - 64 bit support
  - Auto-add
  - DHCP to PXE referral
  - Multicasting

WDS has several requirements for installing the role:

- For both Deployment Server and Transport Server
  - **Active Directory Domain Services** – the server must be a part of a domain or a domain controller, and all forest/domain configurations are supported.
  - **DNS Server** – this component is critical to the operations.
  - **DHCP Server** – WDS uses PXE which relies on DNS to function.
  - **NTFS** – the image store must be an NTFS volume.
  - **Account Credentials** – installation requires local administrative rights.
- Transport Server
  - Server 2008 requires a local admin to install, and does not have a PXE provider, so you must supply one.
  - Server 2008 R2 incorporates a PXE provider in DHCP.

The installation of WDS is accomplished through server manager, and you add the role, just as you would any other. The only install options are to choose the type of services you will install:

- Deployment Services provides full WDS functionality.
- Transport server provides the core networking component used to deploy via multicast.

There are 4 types of WDS images that can be deployed:

- **Boot images** – The boot image contains the WDS client and Windows PE, and provides clients the ability to boot into a minimal environment so image deployment can take place. There is a default boot image called boot.wim in the sources directory of Windows 2008 install media. Custom images can be created with the WAIK tool.
- **Install images** – these images contain an operating system, and are located in the sources directory as install.wim.
- **Discover images** - these images can enable non-PXE workstations through the use of a CD/DVD or USB drive. They allow a static mapping of image location.
- **Capture images** – these images are bootable, and allow the capture of systems into images, that can then be used to deploy to other clients.

To configure basic WDS:

1. Log in with Domain Administrator privileges.
2. Click **Start**, then choose **Administrative Tools**. Click **Windows Deployment Services**. If there is not a server listed under the **Servers** node, right-click the **Servers** node and click **Add Server** to add the local computer.
3. Expand the list of servers in the left pane of the Windows Deployment Services MMC snap-in. Right-click the server and then click **Configure Server**.
4. Follow the wizard through the configuration and then Finish.

WDS can be used to create and capture custom install images. To do this, use the instructions in this section to create a capture image, prepare a reference computer using Sysprep, and then capture the operating system using the Image Capture Wizard.

1. Ensure that there is adequate disk space, that you have logged in as an administrator, and that there is a Boot.wim image on the server.
2. Expand the Boot Images node in the WDS MMC, and right-click one of the image names, and select Create Capture Boot Image.
3. Type the name, description and location for save, and click Finish.
4. To add the image to the server, right click the Boot Image node, and click Add Boot image.
5. Follow the instruction and select the image and you are now ready to boot a client into the capture image, and capture the configuration of the OS.

Now that you have a capture image configured, you will need to prepare a reference computer. Once this has been configured to your satisfaction, you will then create the install image. You will now boot a computer (prepared with Sysprep) into the capture image you have just configured. A wizard creates an install image of the reference computer and saves it as a .wim file. Once this has been captured, it is now ready for deployment.

1. Create a reference computer (install the operating system, applications, and configure).
2. On clients running operating systems earlier than Windows Vista, ensure that you have the correct version of Sysprep.exe on the computer (each OS has its own specific version).
3. Run the command `sysprep /oobe /generalize /reboot` on the reference computer. You can also use the Sysprep graphical user interface by double-clicking Sysprep.exe.
4. When the computer restarts, perform a network boot on the computer by hitting the F12 key.
5. Select the capture image that you created in the preceding procedure, in the boot menu, and then click Next.
6. Choose the appropriate drive, and then provide a name and description for the image. Click Next to continue.
7. Click Browse and then choose a local folder to store the captured install image. Use a local directory to avoid image corruption in the event of a network malfunction.
8. Type a name for the image, using the .wim file name extension, and then click Save.
9. Select Upload image to WDS server.
10. Type the name of the Windows Deployment Services server, and then click Connect.
11. If prompted for credentials, provide a user name and password for an account with sufficient permissions to connect to the Windows Deployment Services server.
12. In the Image Group list, select the image group in which you want to store the image.
13. Click Finish.
14. Now you can PXE boot a client computer to install this image.

**NOTE:** The WDS role cannot be deployed to a computer that used the Server Core installation option.

## Configure Microsoft Windows activation

Microsoft product activation is the process of validating software with Microsoft, and confirms the genuine status of a product, protects from software piracy, and ensures that the product key is not compromised. Activation establishes a relationship between the software's product key and a particular installation of that software on hardware.

All activation methods that are used by Microsoft software are designed to ensure and protect user privacy. Activation data is not traceable to the computer or user, is gathered to confirm that the software is legally licensed.

Licenses for Microsoft Windows products can be obtained through one of three basic channels: retail, original equipment manufacturer (OEM), or Volume Licensing. Each channel has its own method of activation, which is unique. Because companies/organizations can obtain their operating systems through any one of the three available channels, they can choose a combination of methods to activate their software.

You can change your method of licensing through the System Configuration in the Control Panel. Server 2008 also provides a command line utility for licensing both local and remote computers: `slmgr.vbs`. Below are the command line options:

Volume licensing and volume activation use a separate activation technology, and there are two types of keys:

- **Key Management Service (KMS) Key** – This type of key can be used to enable a KMS Server which can be hosted internally, and be uses to automatically activate computers running windows Oss. KMS requires more than 25 computers in a network and PCs authorized by KMS must reconnect every 180 days. A single KMS key can be used to install 6 KMS systems. KNS must be running on Server 2003/2008, Vista or Windows 7.
- **Multiple Activation Key (MAK)** – A MAK is used to activate multiple, or individual computers directly to Microsoft. Once you activate with a MAK, you do not have to reactivate.

Microsoft Volume Activation 2.0 includes the Microsoft Volume Activation Management Tool (VAMT) is and allows companies to manage the activation of their Windows Vista, Windows 7 and Windows Server 2008 computers using Multiple Activation Key (MAK) keys.

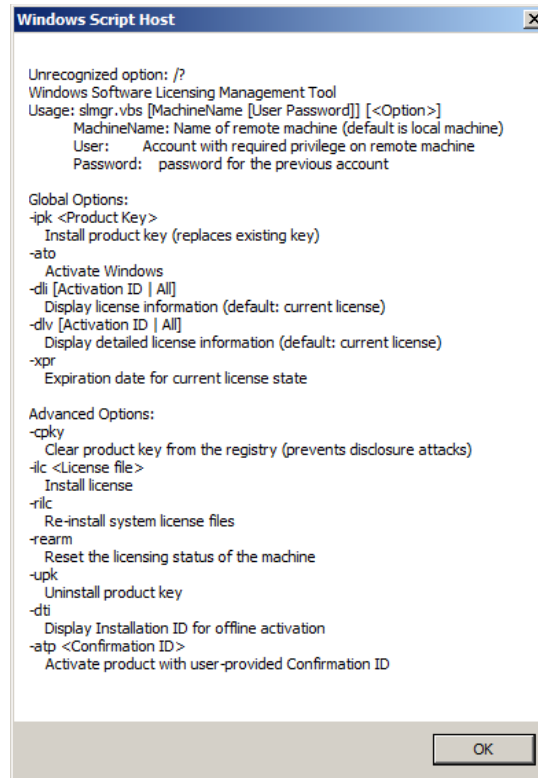


Figure 33: Windows Script Host

Microsoft VAMT version 1.1 enables the following functionality:

- **MAK Independent** - Activation: Each client/server separately connects and activates with Microsoft online or via telephone.
- **MAK Proxy Activation** - Activation of multiple computers with a single online connection to Microsoft.
- **Activation Status** - Provides the activation status of Windows Vista, Windows 7 and Windows Server 2008 computers.
- **Remaining MAK activations** - The remaining activations associated with a MAK key.
- **XML Import/Export** - Allows for the import and export of data to enable activation of systems in disconnected environment scenarios (Done via XML).
- **Local reactivation** - Enables reactivation of computers. This is based on data stored in the VAMT XML computer information list.
- **Configure for KMS activation** - Convert MAK activated volume editions of Windows Vista and Windows Server 2008 to KMS activation.

To install a KMS Host on a Server 2008 machine:

1. Open a command prompt with administrative rights.
2. Enter the following command: **cscript C:\windows\system32\slmgr.vbs /ipk <KmsKey>**  
This will install the KMS Key.
3. Activate the host either through telephone activation or online activation:
  - a. Online - **cscript C:\windows\system32\slmgr.vbs /ato**
  - b. Telephone - **slui.exe 4**

In order to facilitate KMS Activation, manual DNS configuration may be required. Typically, in networks with Dynamic DNS Hosts, computers will publish their available services automatically, and typically the KMS service will publish a SRV record in DNS. If you have hosts that do not support DDNS, or have a default DNS installation, you will need to add SRV records. The reason is that only the first KMS host will be registered with DDNS unless permissions are changed on the DNS server.

To change the default DNS permissions:

1. You must have admin rights in the domain, and all KMS hosts must belong to that domain.
2. In Active Directory, create a globalsecurity group for all your KMS hosts.
3. Add all the hosts to the created group.
4. On the DNS server (s), provide permissions to allow updates by the specified group.  
This will allow SRV record updates.

If you have multiple DNS domains, by default the SRV record will not be published in all of them. You must make a registry entry to facilitate the distribution of the SRV record across all required domains. This can be accomplished through the following on the KMS host:

1. Open regedit and navigate to the following key **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SL**.
2. Enter a new Multi-string value, and enter DnsDomainPublishList.
3. Edit the the multi-string, and enter all of the DNS domain suffixes that KMS should be published to.
4. You must restart the Software Licensing Service when complete.

Within any environment that has hosts that do not support DDNS, you must disable the auto-publishing on all KMS hosts and manually create DNS SRV records using the following steps:

1. In DNS Manager, right-click the forward lookup zone domain, and choose Other New Records.
2. Select the Service Location (SRV) and click create record.
3. You will need to type in the following:
  - a. Service \_VLMCS
  - b. Protocol \_TCP
  - c. Port Number 1688
  - d. Host offering <hostname of KMS>
4. Click Done.

Replication of license data can be done automatically through the use of multiple KMS hosts and the correct utilization of DNS SRV entries.

## Configure Windows Server Hyper-V and virtual machines

Server 2008 R2 Hyper-V is a hypervisor-based server virtualization technology. Virtualization provides great flexibility and management of enterprise applications.

Below are several scenarios that are prime for Hyper-V:

- **Server consolidation** – provides the ability to reduce the amount of hardware, and lower Total Cost of ownership.
- **Business Continuity and Disaster Recovery** – virtualization provides a means to minimize downtime and outages. Disaster recovery provides for rapid re-establishment of business services in the case of a disaster.
- **Testing and development** – a great platform for running multiple instances and version of different technologies.
- **Dynamic Data Centers** – combined with System Center, you can enable dynamic systems and automated reconfiguration.

Key features of Hyper-V in 2008 R2:

- **Live Migration** – is integrated with 2008 R2 and allows you to move virtual machines between host servers without an interruption of service.
- **Increased Hardware Support** – now allows up to 64 logical processors.
- **Cluster Enhancements** – support for the following cluster enhancements:
  - **Cluster Shared Volumes** – CSV allows multiple servers to access SAN storage through a single logical namespace.
  - **Improved Cluster Node Fault Tolerance** – uses dynamic redirection to ensure rapid failover.
- **Network Enhancements** – network performance focus and enhancements improve overall speed of access.
- **Dynamic VM Storage** – provides for the configuration of Virtual Hard Disks while VMs are running.
- **Network Load balancing** – Shares loads across multiple servers.
- **Virtual Machine Snapshots** – allow for restoring of previous states.

## Hardware requirements

Hyper-v requires specific hardware to run, and you need the following:

- An x64-based processor, along with specific x64 versions of Windows Server 2008 Standard, Enterprise and Datacenter.
- Hardware-enforced Data Execution Prevention (DEP) is required and needs to be enabled. On AMD hardware, the AMD NX bit needs to be enabled, and on Intel Hardware, the Intel XD bit must be enabled.
- Hardware-assisted virtualization is required, and available in Intel Virtualization Technology and AMD Virtualization (Intel VT and AMD-V).

## Physical to Virtual Migrations

Physical to virtual migration is the process of taking existing physical servers, and replicating them on the Microsoft Virtual platform. There are two tools provided by Microsoft to make the transfer process seamless:

1. **Virtual Server Migration Toolkit** – VSMT is an older tool that provides a means to migrate NT 4 SP6a, Windows 2000 SP4 and Windows 2003 servers so that they can be hosted under Virtual Server 2005. Once on the 2005 platform, you can then easily migrate to Hyper-v, by using 2005 as a stepping stone. This command line tool provides XML files that store configuration, and allows imaging of machines that can then be virtualized. This tool can be used to migrate older systems, and is really limited to a small number of migration candidates.
2. **System Center Virtual Machine Manager 2008** – this tool not only provides migration capabilities, but can also be used to manage up to 8000 virtual machines, and up to 400 Hyper-v host computers. You can use the application to manage migrations, providing the following prerequisites are met on the hosts:
  - ▶ The target computer has to have ACPI BIOS.
  - ▶ The target requires at least 512MB of memory.
  - ▶ There can be no firewalls between the host and the SCVMM server.

SCVMM can be used on the following Oses: Server 2008, Server 2003 SP1, XP SP2, and Vista SP1.

## Virtual Hard Disks

VHDs store the contents of a virtualized server's storage system, and utilize .vhd files. Typically, a fault tolerant system such as RAID 5 or 10 is preferred, and you can utilize network attached storage, SANs utilizing Fibre Channel, iSCSI or SAS, and direct attach storage. VHDs also provide the ability to emulate either SCSI or IDE. Below is more info on VHDs:

- Virtual guests must use an IDE controller for startup.
- Four virtual SCSI controllers can be utilized within a virtual guest.
- Each SCSI controller can support 64 drive maximum.

There are 3 types of VHDs:

1. **Fixed** – this type of VHD is created at maximum size, and suffers the least amount of fragmentation due to its fixed size. It can be expanded later using the Edit VHD tool.
2. **Dynamic Expanding** – this type of VHD will start at a minimum size, and grow over time to the maximum allocated size. Note: The disk will not shrink if data is removed, and can be compacted through the Edit VHD utility.
3. **Differencing** – when you choose this type of disk, you specify a parent VHD, which is the reference against which all changes are recorded. This allows you to make changes without altering the parent.

Virtual Hard Disks are created through the Hyper-V manager by right-clicking in the Actions Pane, and Clicking New, and then Hard Disk.



## Installing Hyper-V:

On Server Core:

- Verify the latest release version of Hyper-V is installed.
- At the command prompt, type: *Start /w ocsetup Microsoft-Hyper-V.*

To install on a full Server 2008:

- Click Start, Administrative Tools and then click Server Manager.
- In the Roles Summary area of the Server Manager main window, click Add Roles, and then on the Select Server Roles page, click Hyper-V.
- On the Create Virtual Networks page, click one or more network adapters if you want to make their network connection available to virtual machines.
- On the Confirm Installation Selections page, click Install.
- Restart the computer when done and on reboot log on with the same account you used to install the role. After the Resume Configuration Wizard completes the installation, click Close to finish the wizard.

To install Hyper-V on Server Core:

- Perform a Server Core installation – required prior to installing the Hyper-V role.
- After the installation, you need to apply the Hyper-V update from Microsoft. To check on the updates installed, use the following command:
  - `wmic qfe list`
- You will need to see “kbod=950050”, if it is missing, type the following at a command prompt: `wusa.exe Windows6.0-KB950050-x64.msu /quiet` and three updates will run.
- To install the VM Role:  
**start /w ocsetup Microsoft-Hyper-V.**

Just like a physical server, virtual server also require licensing. Below is a description of each Server 2008 version and the number of Virtual Machine licenses (number include with OS purchase):

- Standard – 1
- Enterprise – 4
- DataCenter – Unlimited

Before you configure your first VM, you need to have install media available, know how much memory you will allocate, and determine a naming standard for your machines and storage. Note that the minimum memory requirement for Server 2008 is 512MB, and the max is 8GB/32GB/2TB (Foundation/Standard/Enterprise). Below is a guideline for virtual processors:

- A single-processor/dual-core system provides 2 logical processors.
- A single-processor/quad-core system provides 4 logical processors.
- A dual-processor/dual-core system provides 4 logical processors.
- A dual-processor/quad-core system provides 8 logical processors.
- A quad-processor/dual-core system provides 8 logical processors.
- A quad-processor/dual-core, hyper-threaded system provides 16 logical processors.
- A quad-processor/quad-core system provides 16 logical processors.

Below are the high level steps to configure:

1. In Administrative Tools, click on Hyper-V Manager.
2. In the Action pane, click new, Virtual Machine.
3. Run through the Wizard, and configure the name, location, memory and networking options.
4. You will need to create or direct the wizard at the Virtual Hard Disk.
5. You will finally have the option to install from CD/DVD, ISO, Boot Floppy or the Network.

Creating Virtual Machines is accomplished through the Hyper-V Manager, and from the Action pane, selecting New, then Virtual Machine. Once the machine is created, you can configure all the properties through the properties interface:

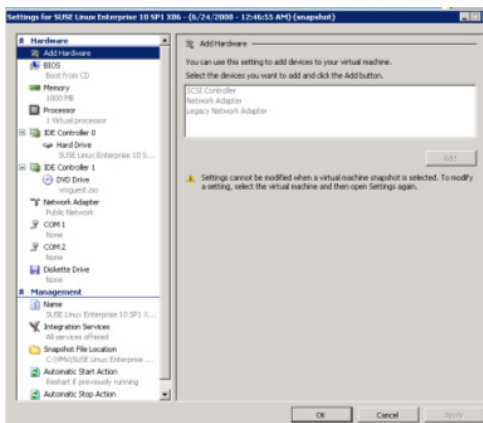


Figure 34: Virtual Machine

To Configure Server Core virtuals remotely through remote desktop, use the following command on Server:

```
cscript c:\windows\system32\scrededit.wsf /ar 0.
```

```
net localgroup administrators /add <user> (add user to admin group to allow connections).
```

This script will enable remote destop connectivity and administration through the host.

## Virtual Networks

With Virtual Machines, also come virtual networks. While Hyper-V allows you to configure complex virtual networks, the basic concept of virtual networking is clear and straightforward. For a simple virtual network configuration, Microsoft recommends that you have at least two network adapters on the Hyper-V server: one network adapter dedicated to the physical machine for remote management and administration, and one+ network adapters dedicated to the virtual machines. If you are operating an Internet SCSI (iSCSI) initiator for VHD storage, Microsoft recommends an additional network adapter is configured within the management operating system. The management operating system is a partition that calls the Windows hypervisor and requests that new partitions are created. There can be only one management operating system. When examining Virtual Networks, there are three types:

- **Private Virtual Networks** – this allows communications between virtual machines on the same physical hardware. This is a network that does not have a virtual network adapter in the management operating system, and is used when you want to isolate the VMs.
- **External Virtual Networks** – this provides the ability for virtual machines to communicate externally and with the management operating system.
- **Internal Virtual Networks** – This is typically used in a test environment, and allows virtual machines on the same physical server and the management operating system to communicate.

## Backups

Hyper-v provides the ability to create a snapshot of a VM, or a backup at a specific point in time. This provides the ability to recover a machine to an exact moment, with all the configuration and running applications, memory state, processes, etc. Snapshot files consist of the following:

- Save state files
- Copy of the VM config file (XML)
- A differencing disk that is the new working disk prior to the snapshot (.avhhd)

To create a snapshot:

1. Click on Snapshots in the Action menu of the Virtual Machine Connection Window, enter a name for your new snapshot, and click Yes. The snapshot will be created and presented in the Snapshots pane of the Hyper-V Manager.

There are two methods to backup Virtual machines:

- Performing a backup from within the Hyper-V host – this can be utilized when you need to backup data from storage not supported by the Hyper-V VSS writer.
- Performing a backup from the Hyper-V host – this can be accomplished when utilizing storage that is Hyper-V compatible, and is also compatible with the Hyper-V Copy Service Writer (VSS).

Online backups can be performed if you are utilizing a Hyper-V aware backup utility, and:

- Integration Services is installed
- The VM does not use Dynamically expanding disks
- All VHDs are NTFS formatted
- Volume Shadow service is enabled on all volumes

## Hyper-V R2 In Windows Server 2008 R2

Windows Server 2008 R2, and therefore exam 70-649, includes changes to the Hyper-V server role. Four of these changes are significant and are likely to be seen on the 70-649 exam:

- **Live migration:** With live migration, administrators may transparently move running virtual machines (VMs) from one node in a failover cluster to another node in the same cluster. During the move, network connections are not dropped and users perceive no downtime. Because failover clustering requires shared storage, live migration requires it as well. In most cases, the shared storage will be implemented with an iSCSI or Fibre Channel storage area network (SAN). The VMs are stored on the SAN, which provides the shared storage. Only one VM live migration can be in progress at a time. You cannot move more than one VM using live migration in one action.
- **Dynamic virtual machine storage:** VMs not support hot removal and hot add (or plug-in) of storage. This means that a new VHD or pass-through disk can be added to a VM without power cycling it. This feature requires that the guest OS be able to support hot swappable drives as well. Hyper-V integration services must be installed on the guest OS for dynamic VM storage to work.
- **Enhanced networking support:** Hyper-V R2 now supports jumbo frames. These Ethernet frames are larger than standard Ethernet frames and can support sizes of up to 9,014 bytes, assuming the physical network supports them. Technically, a jumbo frame is any Ethernet frame larger than 1500 bytes. A standard Ethernet frame, including all overhead, is limited to 1538 bytes without 802.1Q VLAN tagging and 1542 bytes with the VLAN tags. The 1500 byte limit is the limit on the payload size, which is the actual application-useful content in the frame. Jumbo frames are supported in Windows Server OSes, but Hyper-V R2 is the first to support them in a Microsoft VM.
- **Enhanced processor support:** Hyper-V R2 supports up to 32 physical processor cores. A single physical host machine can support many more VMs with this extended processor support. Windows Server 2008 Hyper-V supported 4 sockets and 24 cores or logical processors. Hyper-V R2 supports 8 sockets and up to 32 cores. In addition to the added processor support, you can now use up to 1 TB of RAM, while Windows Server 2008 Hyper-V supported only 32 GB of RAM.

## Configure high availability

Server 2008 includes many features to specifically provide high availability services and applications to the enterprise. Below are the key features:

- **Failover Clustering** – failover clustering provides the ability to automatically switch between servers or virtual server upon a specified failure criteria. Windows Server 2008 R2 expands on previous versions, through improvements aimed at enhancing the overall validation process for clusters, simplified management of clustered VMs (which run with Hyper-V), a new Windows PowerShell, and options for migrating settings from cluster to cluster. Brand new features:
  - ▶ New validation feature - checks system network, storage and system settings to ensure clustering compatibility by running tests during the installation wizard.
  - ▶ GUID Partition Table (GPT) Disk support – GPTs have built in redundancy and can be partitioned to larger than 2 TB.

- **Network Load Balancing** – this feature allows you to spread your application traffic across multiple machines, providing enhanced performance and distribution of traffic load, as well as easy scalability. New features in Server 2008 include:
  - **Improved support for “Sticky Applications”** – allows for persistent connections for applications that require them.
  - IPv4 and IPv6 support.
  - **Improved Health Monitoring and Application and Server Awareness** – provides enhanced means to monitor the health of NLB nodes, allowing for the highest availability.
  - **Ability to support multiple addresses** – NLB now allows multiple IPs.
  - **Integration with ISA Server** – providing enhanced security and the ability to support a mixed IPv4/6 infrastructure.
- **Backup and Recovery** – new features provide the ability to quickly recover systems that fail, incur damage or are lost in a disaster.
  - **Windows Server Backup Tools** – newly redesigned backup and recovery utilities.
  - **Shared Folder Shadow Copies** – ability to snapshot shared resources.
  - **Windows Recovery Environment** – a lightweight OS that provides a simple interface to initiate recoveries.
- **Storage Availability** – provides new features to maintain the ability of storage resources that are essential to IT and Business operations.
  - **Server and storage fault tolerance improvements** – ability to specify primary and alternate storage paths.
  - **Configuration error recovery** – backup and restore capability of storage system configuration parameters to speed recovery in the event of a configuration mishap (or IT blunder).

## Failover Clusters

The following are requirements for enabling Failover Clusters:

### Hardware Redundancy

- Need to utilize a set of 2 matching servers that contain similar or like components. Hardware is supported by Microsoft only if they are marked as certified by Server 2008 R2. All components must pass the validation wizard.
- **Network** – all adapters and cables must be certified. If using iSCSI, you must choose between network based communications or iSCSI, and you cannot use both. Note: you must also focus on redundant network configuration as well as redundant servers.
- **Storage Controllers** – always use like storage device controllers, with the same firmware. You cannot use parallel SCSI connectors. For iSCSI you should use GB Ethernet or higher, and you cannot use teamed network adapters.

- **Storage**
  - ▶ You cannot use dynamic disks, and must use basic.
  - ▶ NTFS volumes only.
  - ▶ You can use either GPT or MBR.
  - ▶ Definition – Disk Witness – this is a disk within the cluster that holds the configuration DB of the cluster.
- **Software requirements** – all servers must run x64 or Itanium architecture, and a single failover cluster configuration must run the same version of Server 2008.
  - ▶ Always run servers at the same patch level.
  - ▶ Only Data Center and Enterprise have Clustering Services (Not std or Web).
- **Infrastructure requirements**
  - ▶ Network settings
    - Always use identical network configuration on each NIC (Speed, Flow Control, Duplex, Media Type).
    - Each adapter requires a unique IP, and should be on a separate subnet.
  - ▶ **Domain Name System** – DNS is required for clustered servers, and you may use Dynamic DNS.
  - ▶ **Domain Controllers** – makes clustered servers member servers.
  - ▶ **Accounts**
    - The account which is used to install the cluster provides the basis from which the cluster account is created.
    - Cluster name account has the same name as the cluster, and is used to create accounts and configure services having to do with the cluster. If this account is deleted, or permissions changed, you will have major issues with the cluster.
    - Clustered Service Accounts – are computer accounts created to match the cluster name.

You can use the Failover Cluster Manager MMC snap-in to validate configurations for failover clusters, create and manage failover clusters, and migrate settings to clusters. You can also configure and manage failover clusters by using Windows PowerShell. The high level steps for creating a Failover Cluster are below:

1. Examine your hardware and infrastructure requirements to ensure compliance.
2. Install the Failover Clustering Feature on all the servers that will participate in the cluster.
  - a. Click on Features in Server Manager, and Add Features.
  - b. Choose the Failover Clustering feature and install.
3. Connect the storage and the networks that the cluster will utilize for operations.

4. Use the Validate Configuration Wizard to examine your hardware and config to confirm compatibility. Make sure you accomplish this on all the servers in the cluster.

The Validate Configuration Wizard consists of five types of tests:

- ▶ **Cluster Configuration** – This test can be run on an existing cluster, and verifies correct configuration.
  - ▶ **Inventory** - Provide an assessment and inventory of the hardware, software, storage and settings on the servers.
  - ▶ **Network** – Validates network settings for clustering.
  - ▶ **Storage** - Examines storage configuration and behavior.
  - ▶ **System Configuration** - Validates system software and configuration settings on the servers.
5. Create the Cluster
    - a. In the Failover Cluster Manager, under Management, click on Create a Cluster.
    - b. Go through the wizard and provide the servers to include in the cluster, the name of the cluster and the IP information.

### Network Load Balancing (NLB)

After configuring and installing hardware for the network load balancing cluster, you can configure the first NLB Cluster Host. The first host acts as the master copy, and can be utilized to create an image using imaging technology. This will ensure that the hosts are configured exactly the same, and reduce manual configuration within the cluster. You can install NLB by using the add features in Server Manager. To install the first NLB Host:

1. Start the Network Load Balancing Manager, and create a new cluster by right-clicking.
2. In the *Host* text box, type the name of the host, and then click *Connect*.

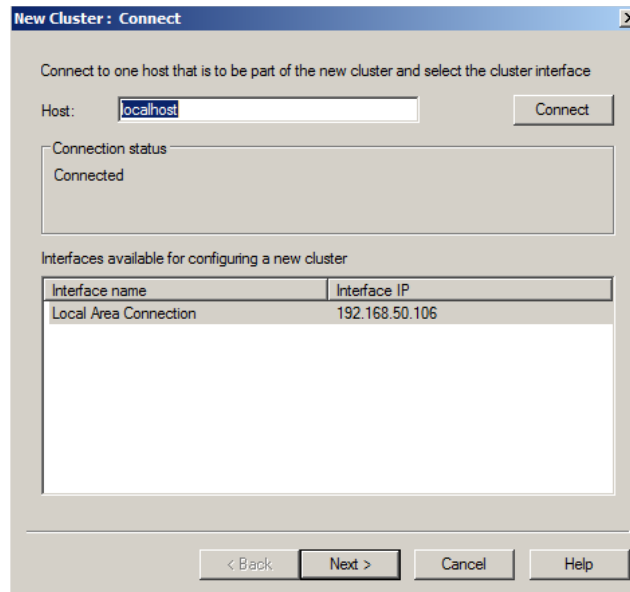


Figure 35: New Cluster: Connect

3. Select the network interface that you want to use with the cluster, and then click *Next*. (The interface will host the virtual IP address and is designated to receive the client traffic to load balance.)

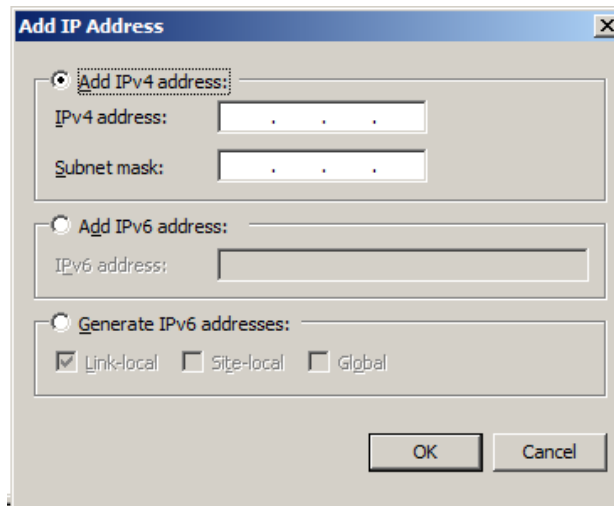
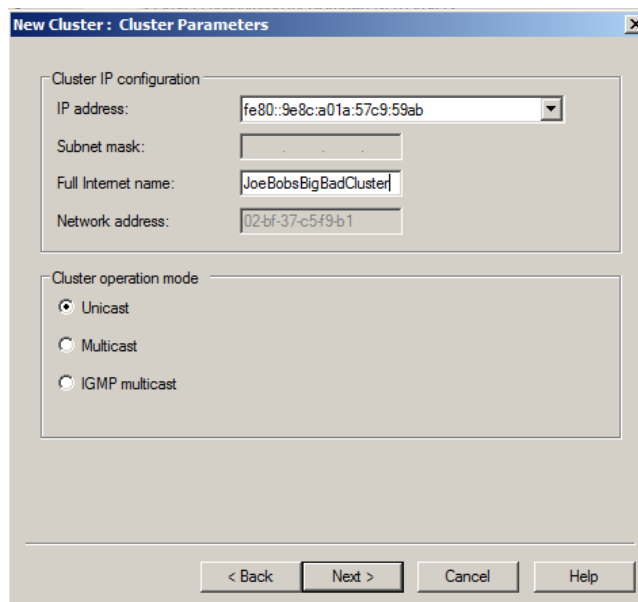


Figure 36: Add IP Address

4. Next, you will set *Host Parameters*, and select a value in *Priority (Unique host identifier)*. This parameter specifies a unique ID for each host in the cluster. All network traffic that is not covered by a port rule will be handled by the host with the lowest numerical priority among the current members of the cluster handles.





**Figure 37:** Cluster Parameters

5. Priorities can be overridden or you can provide load balancing for specific ranges of ports by specifying rules on the *Port rules* tab of the *Network Load Balancing Properties* dialog box.
6. You can also add dedicated IP addresses in *Host Parameters*.
7. In *Cluster IP Addresses*, click *Add* and enter the cluster IP address that will be shared by all hosts in the cluster. This IP address is added to the TCP/IP stack on the selected interface of all hosts that are selected to be part of the cluster.

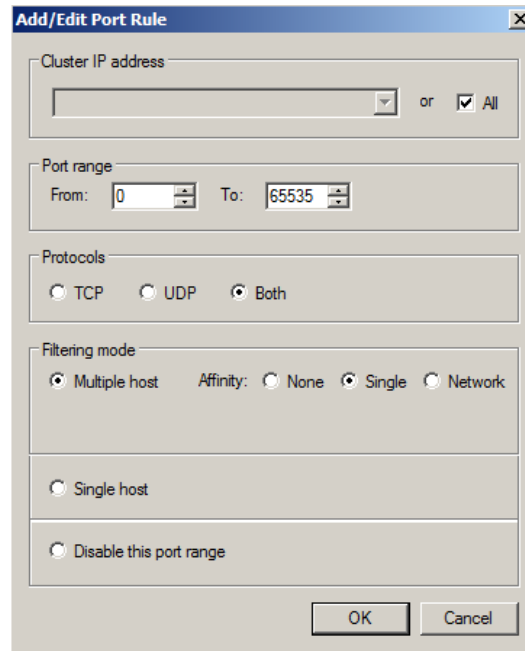


Figure 38: Add/Edit Port Rule

NLB Properties:

- **IP Address** – this is the cluster’s primary IP. This should be the IP that has a hostname mapped for the cluster.
- **Network address** – specifies the MAC of the network adapter used for client to cluster connectivity. This is a virtual MAC, and the server will change its burned in address to this to enable cluster connectivity.
- **Cluster Operation Mode** – this allows you to enable multicast mode for the cluster. Enabling IGMP support will limit multicast broadcast through switches.
- **Port Rules** – allows you to add filtering rules on which port ranges the cluster will provide services.
- **Affinity** - is applicable only for the Multiple hosts filtering mode. Think of affinity as “stickiness” when it comes to connections. There are several affinity choices:
  - ▶ *None* - provides that multiple connections from the same client IP address can be handled by different cluster hosts). Avoid using None when selecting UDP or Both for your protocol setting, otherwise traffic will be fragmented.
  - ▶ *Single* - NLB will direct multiple requests from the same client IP address to the same cluster host. This is the default setting.
  - ▶ *Network* - NLB will direct multiple requests from the same TCP/IP Class C address range to the same cluster host. Enabling Network affinity ensures that clients that use multiple proxy servers to access the cluster have their TCP connections directed to the same cluster host.

“The use of multiple proxy servers at the client’s site causes requests from a single client to appear to originate from different computers. Assuming that all of the client’s proxy servers are located within the same address range, Network affinity ensures that client sessions are properly handled. If you do not need this capability, use Single affinity to maximize scaled performance (*Microsoft TechNet*).”

- ▶ As an added feature to the Single and Network options, you can configure a time-out setting to preserve client affinity.

**Note:** Affinity should only be utilized when necessary and will not be the best configuration for max performance.

## Configure storage

RAID provides redundancy through the use of multiple physical disks that are used to create a logical disk volume. Windows server 2008 provides support for RAID 0, 1, and 5 through software. An overview of RAID levels are below:

- **RAID 0** – Also known as striping, this RAID level lets you utilize 2 or more disks, and combine them into one single volume. The drawback to this level is that there is no redundancy, and if you lose a single disk, the entire volume of data will be lost.
- **RAID 1** – Also known as Mirroring, two disks are utilized, and are exact copies. If one fails, the other can immediately take over and provide services. This is typically used as the volume to store the operating system, and provides redundancy.
- **RAID 5** – This level requires a minimum of 3 disks, and is an enhancement to striping, through the use of a parity disk. This level allows for a single disk failure, whereas the parity drive takes over for the failed hardware.
- **RAID 10** – Also called a striped mirror, this combines RAID 1 and 0 to create a large, fast volume. It requires at least four drives, and is only supported by hardware RAID devices.

In order to use any of the expanded capabilities within Server 2008 Storage management, the volumes must be dynamic. Dynamic volumes support RAID and spanned volumes. A spanned volume consists of drive space spread over more than one physical disk, and you can span simple volumes that are not system or boot volumes, and can create them on dynamic disks as well. (Remember, a spanned volume may or may not go across physical disks, whereas RAID utilized multiple drives).

Striped volumes can be created only on dynamic disks, and cannot be extended after creation.

Note: you can use up to 32 volumes to create a striped disk within windows.

Note: Microsoft provides a full command line tool DISKPART that can be utilized to perform all different types of disk management functions, including RAID creation, formatting and the ability to change disk volume types. This tool can be quite handy when you may have a non-bootable system that needs some disk work.

To Configure Disk Mirroring (RAID 1):

1. Open Server Manager, and select the Storage Node.
2. Click on Disk Management.
3. Ensure that you have a disk volume of equal size to Disk 0, and that it is online.
4. Right-click Disk 0, and choose Add Mirror. You will be prompted to select the Disk which will become the mirror.
5. It will take some time to synchronize the mirrored disk.

To Configure RAID 5:

1. Open Server Manager, and select the Storage Node.
2. Click on Disk Management.
3. Make sure that all of your volumes are online, and then right-click the first unallocated volume and choose New RAID 5 volume. This will start the RAID wizard.
4. Add all the participating disks, and set the size.
5. Choose the drive letter, and then format.
6. After formatting, the disks will be labeled as a RAID 5 volume.

## Virtual Disk Service (VDS) APIs

Server 2008 provides a whole set of scripting tools and application programming interfaces (APIs) that allow command line management and configuration options for both physical and virtual disks. Many of these commands have been incorporated into a wide variety of command utilities, the main one being diskpart. DISKPART that can be utilized to perform all different types of disk management functions, including RAID creation, formatting and the ability to change disk volume types. In 2008 the tool has also incorporated many virtual disk functions including:

- **Create vdisk** – allows the creation of a new VHD.
- **Attach/detach vdisk** – provides mount and unmount functions.
- **Expand vdisk** – expands a vhd.
- **Merge vdisk** – merges a differencing disk with its parent.

## SANs

Server 2008 provides Storage Manager for SANs to help manage Storage Area Networks, and give administrator configuration capability on iSCSI and Fibre Channel drive systems. A LUN is a logical reference to a storage subsystem or portion of that system. There are several different LUNs supported in Server 2008:

- **Simple** – only use a single drive or portion of a drive.
- **Spanned** – spans multiple drives.
- **Striped** – write data across a number of physical drives. This type of LUN speeds up performance, but provides no fault tolerance, and cannot be mirrored or extended.
- **Mirrored** – creates identical copies of 2 physical drives.
- **RAID 5 / Striped with Parity** – Fault tolerant and require 3 or more disks.

There are several requirements for creating LUNs:

- The Virtual Disk Service (VDS) must be supported.
- VDS Hardware provider must be installed.
- The required storage space must be available.
- Server connections for the LUNs must be configured in Manage Server Connections.
- Any LUNs being added to a cluster must have a cluster established.

Windows Server 2008 provides Storage Manager for SANs to provide an administrative interface for managing and configuring iSCSI or Fibre Channel SANs. The Storage Manager can be installed through the following steps:

1. Open Server manager.
2. Click on the Features node, and select Add Feature.
3. Choose Storage Manager for SANs.

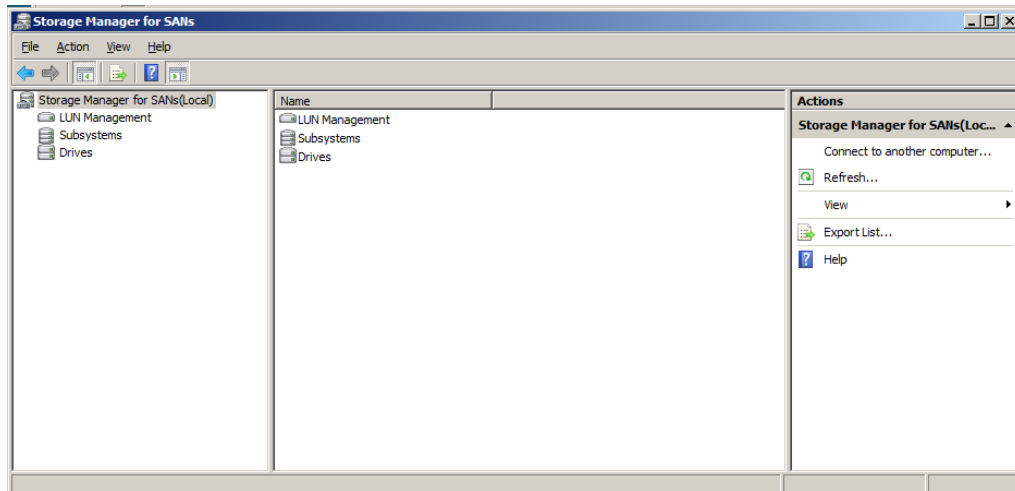


Figure 39: SANs

Storage Manager for SANs can be utilized to perform a number of functions:

- Create, extend and delete LUNs
- View the properties of installed iSCSI and Fibre Channel storage systems
- Assign servers and clusters LUNs
- Manage host bus adapter ports (HBAs)
- Manage iSCSI settings
- Monitor LUN health and status

Configuring these items is fairly simple and is managed through right-clicking the parent node in Storage Manager, or right-clicking the item, such as a LUN and then choosing the action to perform. In order to manage and configure storage subsystems, you must install the Virtual Disk Service (VDS) hardware provider (compliant with 1.1 standard).

## SAN Technologies

**Fibre Channel** is a widely deployed SAN technology that provides a high performance connectivity to storage devices. Fibre Channel utilizes special switching technology between the servers and storage devices to remove contention normally seen with SCSI type storage devices. Fibre Channel hardware is very proprietary, and it requires special hardware, HBAs, cabling and switches.

**iSCSI** is a SAN protocol that utilizes TCP/IP to transmit information from initiators to storage devices. iSCSI does not require special hardware or cables to function, and has a simplified configuration whereas LUNs are assigned iSCSI targets (connections to storage hardware). iSCSI is managed through the iSCSI initiator in the Administrator Tools. To connect to an iSCSI target:

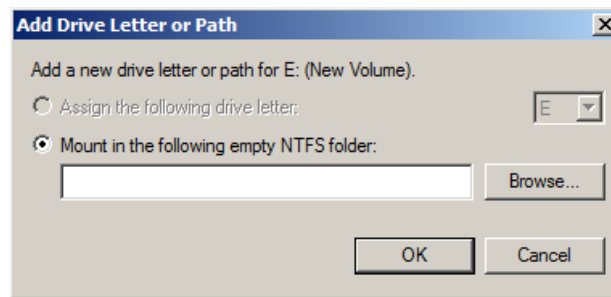
1. Open the iSCSI initiator in the Administrator Tools.
2. On the Discovery tab, click on Add Portal and enter the IP of the iSCSI target.
3. Once this is done, you can click on the Targets tab and see all of the discovered target devices. You can choose to log on, and connect.
4. Once this is established, you can now set Volumes and Devices in the tab of the same name.

## Mount Points

Disk Management in Server 2008 provides the ability to assign a mount-point folder path, rather than a drive letter, to a drive.

To assign a mount point in Disk Manager:

1. Right-click the volume or partition, and then click on Change Drive Letter and Paths.



**Figure 40:** Add Drive Letter or Path

2. Browse to the correct folder, and click Ok.

To add a mount point using diskpart:

1. Open a command prompt and type diskpart.
2. Type list volume, and choose the volume number.
3. Type select volume <volume number>.
4. Type assign [mount=<path>].

## 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 of 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. You can even 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.

**Figure 41:** WAIK Tools

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 70-649 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. It cannot be used to deploy VHDs to virtual machines, but 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.

**Figure 42:** WDSUTIL Parameters

## 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).

## Configuring Terminal Services

Terminal Services within Server 2008 has been greatly improved, and can provide vast benefits to the corporate enterprise, including:

- Rapid deployment of applications and patches through centralized administration and the controlled TS environment.
- Reduction in the use of network bandwidth due to high requirement applications.
- Increase in productivity by providing access to the Windows Desktop from any location.
- Improved performance in branch offices due to the minimized data transfer requirements.

Terminal services is comprised of a server role that can be added to a server, along with multiple role services:

- Terminal Server – allows the server to host the full Windows desktop or any windows based application.
- TS Licensing – manages all licensing functions within the terminal environment. All client access licenses are stored here.
- TS Web Access – provides access to RemoteApp and Remote Desktop through a Web interface.
- TS Gateway – provides access to terminal resources through the Internet.
- TS Session Broker – provides load balancing of terminal services connections.

Below is an overview of the TS installation steps:

1. Go into Server Manager and install the Terminal Services Role.
2. When installing TS, you will be prompted to choose which role services you need:

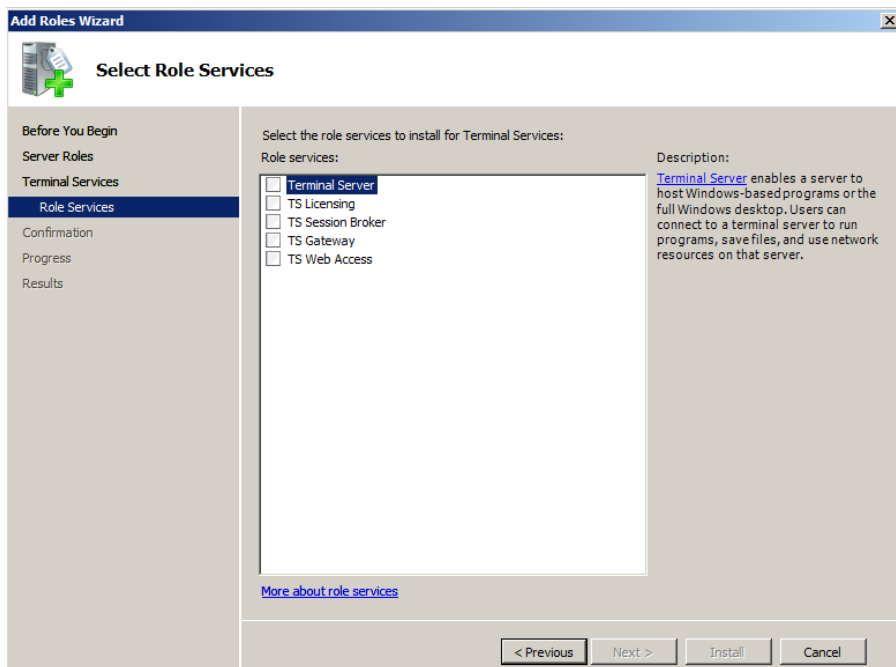
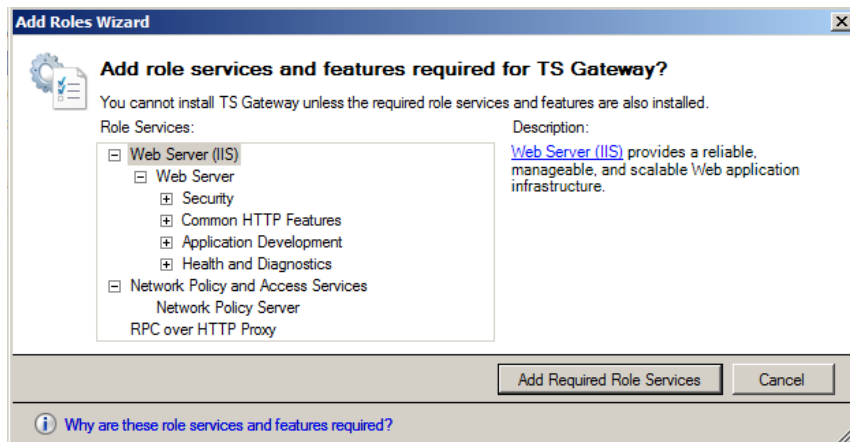


Figure 43: Select Role Services

**Note:** When you add TS Gateway, you will be prompted to install numerous additional services, including the ones seen below:

3. You will then be prompted to select/ choose whether or not to require Network Level Authentication. This is a new authentication method that requires network authentication before a remote desktop session can be established.
4. Next you will choose how to license the TS, and you have several options:
  - a. Configure later
  - b. Per Device – requires a CAL for each client device that accesses the TS
  - c. Per user – licensing is specific to users



**Figure 44:** Add Roles Wizard

5. Specify the groups that can access the terminal server.
6. Next you will specify the discovery scope for the license server. This defines the scope of TSs that can discover this license server and can be set to the overall domain, or the forest. You also have the ability to set the location of the TS licensing database on this screen.
7. If installing the TS Gateway, you can specify SSL options, and enter certificate information.
8. You will be prompted to identify NAP servers.
9. Finish.

## Configure Windows Server 2008 Terminal Services RemoteApp (TS RemoteApp)

TS RemoteApp programs can be run from a remote client through the terminal services environment, just like they are running on the local computer. TS provides the ability to run multiple RemoteApp sessions through a single terminal session, reducing overall licensing. Remote App is suited for:

- Remote application access.
- Branch offices with limited network connectivity and no local IT.
- Custom Line of Business Application Access and Deployment.
- Hot desk environments, where users do not have their own computers, or share a workspace.
- When multiple versions of apps are required.

There are several options on how to run Remote App:

- TS Web Access can be utilized through a link to the RemoteApp program.
- Administrators can create custom RDP files with the .rdp extension that can be distributed to end users require application access.
- Apps can be distributed through .msi packages, and will show in the start menu.
- File extension associations can be configured, and users can just click on an associated file.

An overview of the steps required to configure an installed app to run through TS RemoteAPP. This is accomplished on the server through the following procedure:

1. Open the TS RemoteApp Manager.
2. In Actions, click on Add RemoteApp programs, and the wizard will start.
3. Check the boxes for the applications you would like to add.

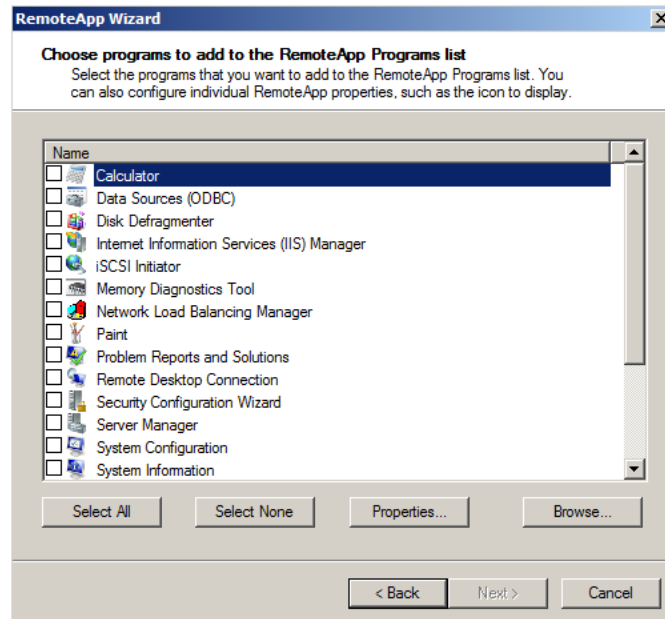


Figure 45: RemoteApp Wizard

Once remote apps are added and configured, you will see them within the Server Manager TS Remote App Manager interface:

RemoteApp Programs			
Name	Path	TS Web Acce...	Arguments
Calculator	C:\Windows\System32\calc.exe	Yes	Disabled
Paint	C:\Windows\System32\mspai...	Yes	Disabled

Figure 46: RemoteApp Programs

To further configure applications, choose to show in TS Web Access, or create RDP/Installers, just Right-click or select options in the Action pane.

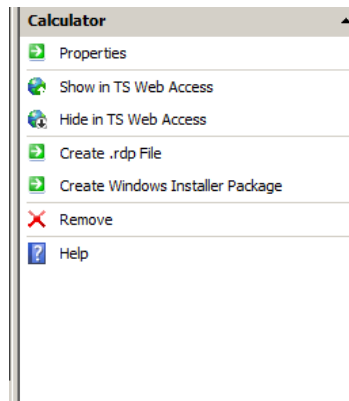


Figure 47: Calculator

Once applications are configured, you will need to right-click the TS-RemoteApp Manager node in Server Manager, and choose Terminal Server settings. This dialog provides a full set of configuration options for RemoteApp deployment and configuration. To enable remote desktop connections over TS Web Access, you must check the “Show a remote desktop connection to the TS in TS Web Access” check box, as seen below on the Terminal Server Tab. Web access provides universal access through a standardized port (80) and a universally adopted protocol set, and allows for simplicity in firewall port settings.

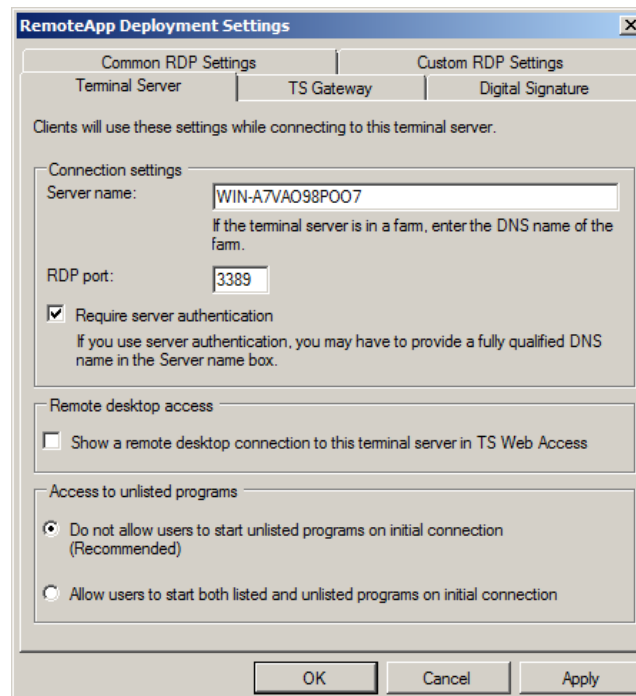


Figure 48: RemoteApp Deployment Settings

## Configuring Terminal Services Web Access

Once TS Web Access has been installed on a Windows Server 2008-based Web server, users can connect to the TS Web Access server to access RemoteApp programs that are hosted on a Windows Server 2008-based terminal server. TS Web provides many benefits, including the following:

- If a user starts more than one RemoteApp program through TS Web Access, the RemoteApp programs run within the same Terminal Services session, minimizing licensing requirements (note, they need to be running on the same terminal server).
- With TS Web Access, applications are easily deployed from a central location. Programs are running on the terminal server and not on the client computer, so upgrades and patches are simple to roll out.
- Users can access RemoteApp programs from a Web site over the Internet or from an intranet.
- Remote Desktop Web Connection enables users to connect remotely to the desktop.
- TS Web Access requires minimal configuration. The service also includes a web part that can be easily integrated into SharePoint implementations.

Requirements for TS Web Access:

- Windows Server 2008
- IIS 7
- The server does not need to be a terminal server
- TS Web Access requires RDC 6.1, which is included with Server 2008, Vista SP 1 and XP SP 3

To install TS Web Access you must perform the following steps:

1. Install the .Net 3.0 Framework.
2. Install SharePoint Services 3.0 SP1.
3. Register the Web Part's namespace and assembly by editing the following file:  
C:\inetpub\wwwroot\wss\VirtualDirectories\80\web.config

Add the following:

```
<SafeControl Assembly="TSPortalWebPart, Version=6.0.0.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35" Namespace="Microsoft.TerminalServices.Publishing.
Portal"
TypeName="*" Safe="True" AllowRemoteDesigner="True" />
```

4. Create a folder and assign permissions for the web part images.
5. Add the Web Part to your SharePoint site through the use of the Edit Page and Add Web part functionality in Site Actions in SharePoint.

## Configure Terminal Services Gateway

The TS Gateway provides many advantages:

- It allows remote users to connect to internal corporate network resources through an encrypted network connection, without the requirement of a virtual private network (VPN) connection.
- It provides an enhanced security configuration model that enables total control over internal network resources. It also provides a point-to-point RDP connection, reducing the risk of full internal network access.
- Remote users are able to connect to internal network resources that are hosted behind security devices/firewalls in private networks and across network address translators (NATs) with minimal configuration. TS Gateway transmits RDP traffic to port 443 instead of 3389, through the use of a SSL tunnel.
- The TS Gateway Manager allows you to configure authorization policies to define conditions/ rules that must be met for remote users to connect to internal network resources. For example, you can specify:
  - Who can connect to the network.
  - What internal resources they can access.
  - Group permissions.
  - Whether device and disk redirection is allowed (Leap frogging).
  - Whether clients have to use smart card authentication or password authentication or a combination of the two.
- TS can be configured to use Network Access Protection (NAP) to further deepen security.
- TS Gateway integrates seamlessly with Microsoft Internet Security and Acceleration (ISA) Server to enhance and expand security.
- TS Gateway Manager provides an enhanced toolset monitor, report and provide auditing capability.

TS Gateway requirements:

- Server 2008.
- Administrative rights required for installation.
- You will need an external SSL Certificate for the TS Gateway. By default, the server uses TLS to encrypt data transmissions. In addition, the cert must meet the following requirements:
  - You need to match the certificate name, CN, to the DNS name of the server/.
  - The cert must be a computer cert.
  - The Enhanced Key Usage (EKU) of the server certificate must be Server Authentication.
  - Cert must have a private key, and must be valid.
  - The certificate must be in the Trusted Root Certificate Store on the clients.

## Install and TS Resource Authorization Policy (RAP) Config

Below is an overview of the installation steps to install and configure TS Gateway:

1. Install the TS Gateway Service Role.
2. Obtain a certificate for the Gateway Server.
3. Configure a certificate for the server.
4. Create a TS connection authorization policy (TS CAP).
  - a. TS CAPs allow you to specify who can access a TS environment.

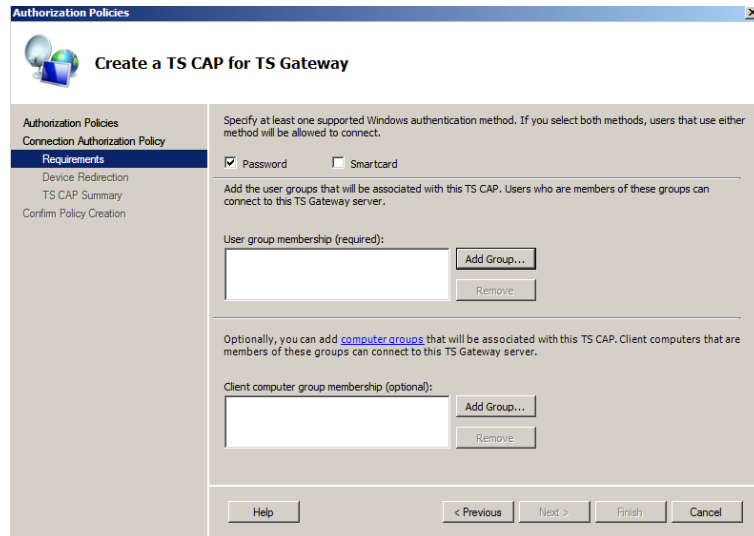


Figure 49: TS CAP for TS Gateway

5. Create a TS resource authorization policy TS RAP.
  - a. TS RAPs let you specify the internal resources that TS users can access.

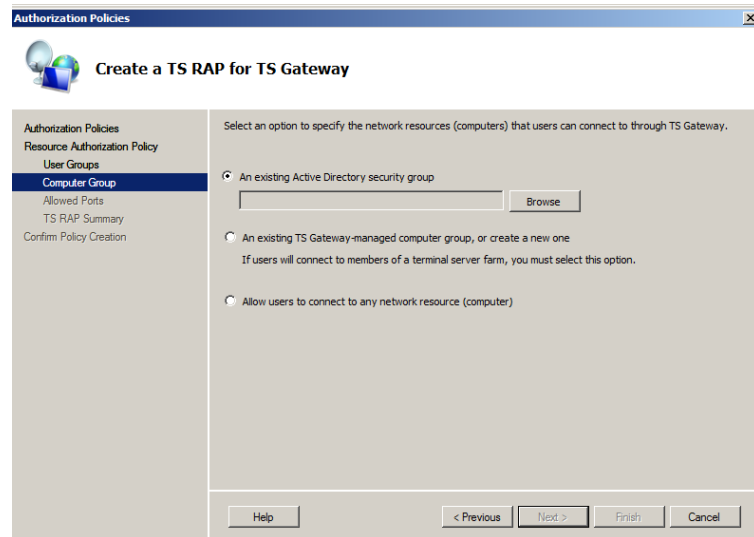


Figure 50: TS RAP for TS Gateway

6. Provide connection limits if required.



## Policy Configuration and Customization

TS RAPs/CAPs are configured within the TS Gateway Manager node, under the specific server, within the policies node. The central TS policy store is configured under the Server properties, on the TS CAP Store tab. You can configure the store to be stored locally on the local Network Policy Server, or stored on a central NPS. The steps to create a policy are fairly simple, and noted above within the initial configuration steps.

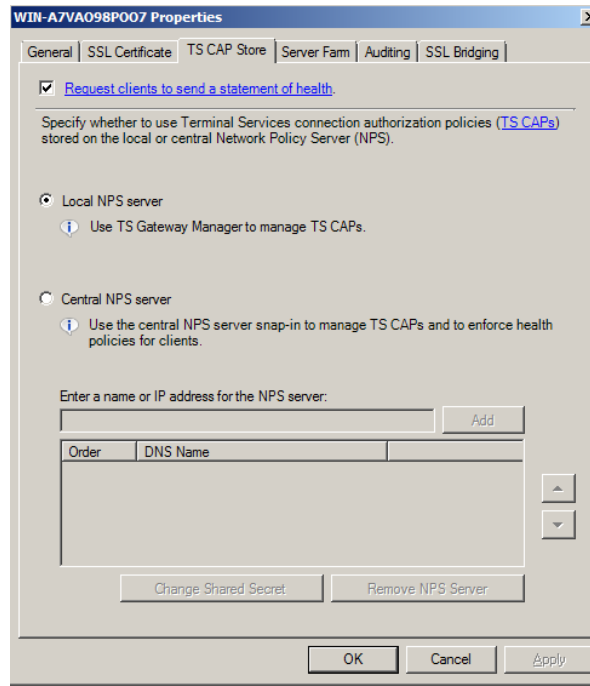


Figure 51: TS CAP Store

## Certificate Configuration

The TS Gateway requires an externally trusted SSL certificate, and utilizes the cert to provide encryption through the Transport Layer Security (TLS) 1.0 provider, encrypting all traffic between clients and the gateway server. The certificate is installed on the gateway, and you do not need a Certificate Authority infrastructure to produce the cert. It can be a self-signed certificate as well. The certificate must meet the following requirements:

- The subject line of the certificate, or CN, must be the DNS name of the server.
- It must be a computer certificate.
- The Extended Key usage, or EKU, must be server authentication.
- It has to have a private key.
- Specific key usage values must be set.
- It must be trusted on the clients.

To configure a certificate for usage:

1. Open Server Manager, Select the Terminal Service Role node, and choose TS Gateway Manager.
2. Right-click the server, and choose properties.
3. Select the SSL Certificate tab, and either select an existing, or create a self signed cert.

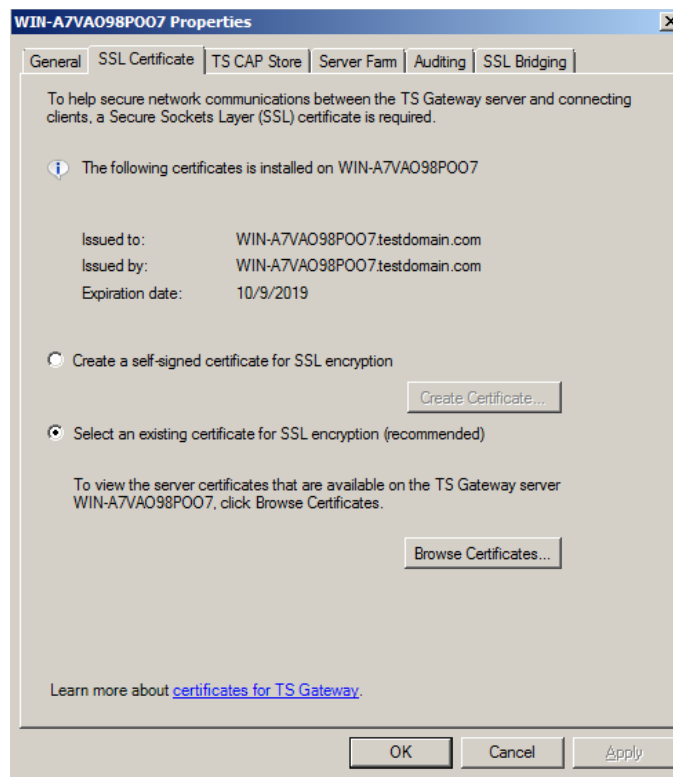


Figure 52: SSL Certificate

## Terminal Services Group Policy

Server 2008 has expanded the configuration options to control TS through group policy tremendously, below is an overview of the configuration options available through Group Policy Configuration:

**Computer Configuration\Policies\Administrative Templates\Windows Components\  
Terminal Services**

## Configure Terminal Services load balancing

The TS Session broker service provides the ability to load balance TS sessions across multiple servers within a farm, and will automatically provide reconnection and redirection for users with existing sessions. The TS Session Broker load balancing function provides two phase functionality:

- First, initial connections are directed through DNS Round Robin.
- After authentication, the TS Session Broker decides how to route/redirect the user to the appropriate server that houses the existing session.
  - If a user has an existing session, redirection takes place to the server where the session exists.
  - If no session exists, the user is directed to the server with the fewest connections.

Load Balancing also has some specific characteristics with TS:

- There is a maximum of 16 pending logon requests.
- You can assign weighted values to servers to ensure more powerful hardware receives the most connections.
- A “server draining” feature is provided to slowly eliminate connections by denying new connections.

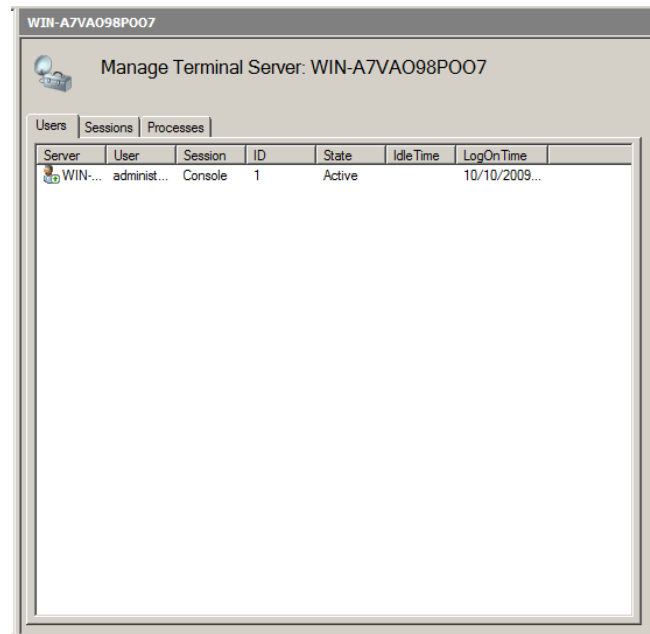
Tasks required for providing TS Session Broker Load balancing:

1. Install the TS Session Broker role service through the Server Manager. It is recommended not to install the service on a Terminal Services Server so that any required maintenance on TS will not affect incoming connection or the functionality of the service.
2. Add all the TSs in the farm to the local Session Directory Computers group on the Broker Server.
3. Configure each terminal server to join the session broker farm and participate in the Broker Load Balancing.
4. Configure the DNS servers to perform round robin. This can be accomplished through the creation of multiple A records.

## Configure and monitor Terminal Services resources

Monitoring TS within a Server 2008 can be an arduous task because of the different layers. Picture that you have the host system and all the processes running, and then each of the individual users and sessions, all with separate processes.

Terminal Services comes with a wide variety of tools to monitor and track connections, as well as performance monitoring. Each of the Role services provides a quick view of status and any problems through their respective MMC plugins in Server Manager. TS Manager is the best place to start, and provides a quick overview of the Users connected, existing sessions and processes with regards to TS. You can configure the refresh interval of this interface by right-clicking the TS Manager node, and choosing the refresh interval for processes as well as status dialog boxes.



**Figure 53:** TS Manager Quick View

TS Gateway Server provides specific information about active connections and their session information. Information provided includes: Connection ID, User ID, Username, Time connection established, Connection Duration, Idle time, Target Computer, Client IP, and target port. All of this information can be viewed through the TS Gateway Manager snap-in, in the monitoring node.

TS Gateway also provides an Auditing function that will allow you to log specific event types into the windows event log. Auditing is enabled through the use of the Auditing tab found in the Server properties within TS Gateway Manager. The following events can be logged:

- Successful user disconnection from resource
- Failed user connection to the resource
- Failed connection authorization
- Failed resource authorization
- Successful resource connection
- Successful connection authorization
- Successful resource authorization

These events are then logged within the event viewer under Application and Service Logs\Microsoft\Terminal Services Gateway.

Performance Monitor provides three separate counter sets to view TS information:

- Terminal Services Gateway – allows connection and authorization tracking.
- Terminal Services – overall session tracking- active, inactive and totals.
- Terminal Services Session – this counter set by far has the most granular tracking capability, and provides the ability to track all types of session specific performance information, including: processor allocation, input and output stats, memory counter and specific TS functions.

## Allocating resources by using Windows Server Resource Manager

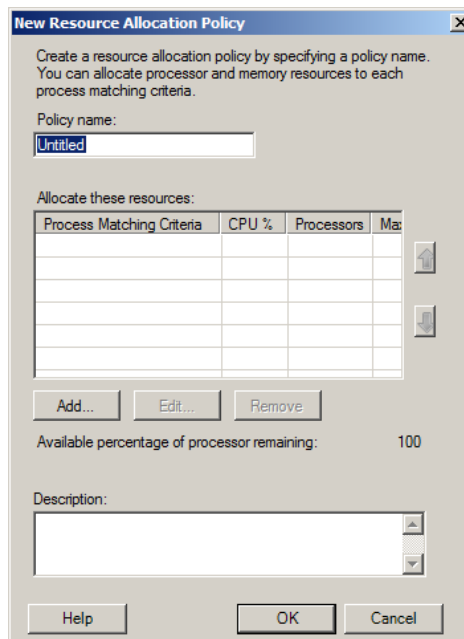
Windows Server Resource manager (WSRM) provides the ability to manage and monitor server processor and memory allocation and usage. This allows you to split resources either equally, or in a biased manner depending on requirements. In a Terminal Server environment, this provides great control and flexibility. To install WSRM:

1. In Server Manager, click on Add Features.
2. Select Windows Server Resource Manager and choose the defaults. Note WSRM requires the Windows Internal System Database.

To start WSRM and configure, go to Administrative Tools and choose WSRM. You will need to connect to the local computer. There are two specific Resource Allocation Process Policies for Windows Terminal Services, and they are: Equal\_Per\_Session and Equal\_Per\_User (Session is new to 2008). To configure and implement an Equal\_Per\_Session policy, right-click the Equal\_Per\_Session node and Set as Managing Policy. This will now provide resource sharing according to TS sessions.

To create a new Resource Allocation Policy:

1. Right-click the Resource Allocation Policies node, and choose new.
2. Enter a name for you new policy and click Add.



**Figure 54:** New Resource Allocation Policy

3. Once you click Add, you can now add process matching criteria, and set CPU and memory allocations for specific processes, services, applications and IIS App Pools.

Monitoring the resources can be accomplished through the following means:

- Clicking on any of the resource allocations policies will provide a quick view into the processor and memory states.
- Clicking on the Resource Manager node will show overall CPU usage, as well as managed CPU cycles and process specific usage.

## Configuring application logging

Terminal Services has a variety of logs that can be checked for troubleshooting and auditing. When you install the specific TS roles, you will get Application and Services logs within the event viewer specific to Terminal Services. Additionally, the Terminal Service Gateway provides enhanced application logging, and this can be configured in the Properties Dialog of this role. Below is a screenshot of the auditing options:

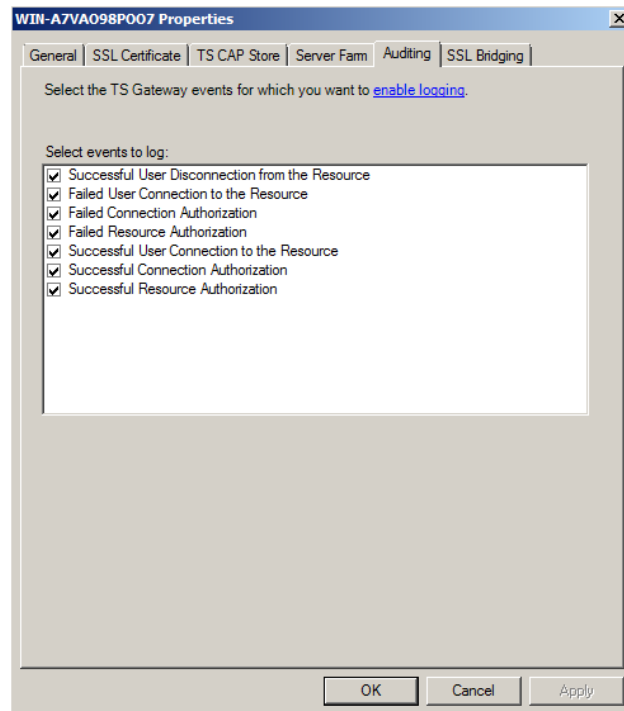


Figure 55: Configuration Application Logging

## Configure Terminal Services licensing Deploying licensing server and Managing CALs

The Terminal Server provides access to applications running on a server. As clients connect, the TS License Server makes the determination if the client needs a TS Client Access License (CAL), and then delivers the license and manages the entire process. These CALs are stored on the License Server, and are assigned to both devices and users, depending on the application and requirement. The License Server function is totally separate from the Terminal Server itself, and may be located on the Terminal Server, or on a separate dedicated server. The TS License Service is very low impact, and requires minimal memory, CPU and bandwidth. So a single server can handle a large number of clients.

Terminal Services provides a separate role for its licensing function: Terminal Services License Server. The license server is the storage entity for the different types of client access licenses (Device and User) installed for a group of Terminal Servers, and provides overall management and control. The License Server can be a separate server, or the role can be installed on a Terminal Services Server. The TS License Server provides these features and benefits:

- Allows minimal impact on networks and servers by offloading the licensing function
- Provides tracking and reporting for the TS Licensing function
- Centralized administration
- Support for all licensing programs and types

There are several ways to set the TS licensing mode:

- When adding the TS role, you can specify the licensing mode, and may choose to configure the mode later. The two modes, Per User and Per Device, are utilized in differing environments. The Per User CAL allows a single user to access an unlimited number of computers/devices. The per device CAL provides a single device access, and are usually used when a single computer is used by multiple users.
- You can set the mode through the TS configuration tool. Note: this option will be grayed out if you have set the licensing mode in Group Policy.
- You can utilize the Set Terminal Services licensing mode within Group Policy in Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Licensing.

All licensees provide a 120 day grace period, and clients can connect within that time without a permanent CAL. Activation of licenses can be accomplished through three different methods:

- **Automatic Connection** – this method works like the standard windows activation, and requires SSL.
- **Web Browser** – you can utilize a web browser to activate.
- **Telephone** – You can call MS Support to activate licenses as well.

To activate the license server, open up the TS Licensing Manager, right-click on the server you would like to activate, and choose Activate Server. You will choose your activation method above, enter company information, and then finish the wizard. Once this is complete, you can choose to install your client access licenses.

During installation of the TS License Server role, you are prompted to choose the discovery scope for your license server implementation. The choice of scope options depends on whether you are a member of an Active Directory Domain, and are as follows:

- **Workgroup** – this options is only available to servers that have not yet joined a domain. It allows local workgroup TS servers to auto-discover the server. Note: If you add the server to a domain or make it a domain controller, Windows will automatically change the scope to domain.
- **Domain** – When you choose the domain scope, and the LS is installed on a Domain controller, servers will automatically discover this licensing entity. The installation/configuration account is required to be a Domain administrator if you want to choose this role.
- **Forest** – when you choose this scope, the service is automatically published as an AD Domain Service, and thus can be discovered by any server in the forest.

CALs can be managed through several interfaces:

- **Terminal Services Configuration** – provides an overview of the license directory, mode and discovery modes, as well as licensing diagnostic information. It also shows all the discovered license servers on the network, how they were discovered and any issues they may have.
- **TS Licensing Manager** – provides the interface to license and connect, as well as a full reporting engine, and method to activate licenses.

- **Group Policy** – provide the means to manage the issuance of licenses. You can control which terminal servers are issued licenses through the Following Group Policy Setting:

**Computer Configuration\Administrative Templates\Windows Components\Terminal Services\TS Licensing**

You set the License Server Security Group, the server will only hand licenses to members.

Note: The license server needs to be a domain member for you to add computers to this group.

## Connectivity between terminal servers and Terminal Services licensing server

A terminal server must have the capability to contact or discover a TS license server in order to facilitate the licensing process and allocate Terminal Services client access licenses (TS CALs) for users and/or computers that are connecting to the terminal server.

The license server discovery mode for the terminal server can be set in the following ways:

- Through configuring the License Server discovery mode in the Terminal Services Configuration tool. This can be done within the Licensing section:

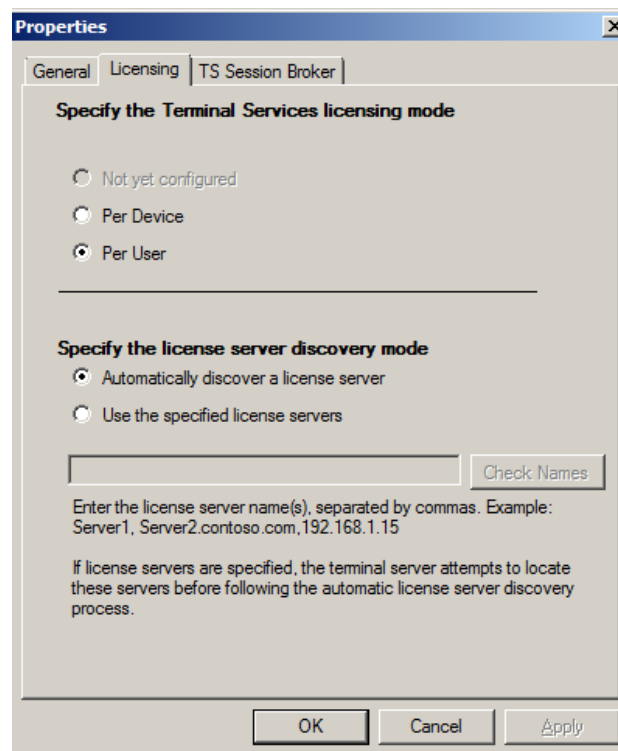


Figure 56: Licensing

- If the Specify the license server discovery mode options are grayed out and you cannot make a selection, then group policy is preventing this setting, and you must change the Use the specified Terminal Services license servers Group Policy setting.



This Group Policy setting is located in **Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Terminal Server\Licensing** and must be configured by using the Group Policy Management Console (GPMC). **Note:** This Group Policy setting will override the setting configured in Terminal Services Configuration.

## Recovering TS LicenseServer

In order to facilitate a backup in the case of system failure, and the ability to recover TS CALs, you must backup the system state as well as the TS License Database. You can find the location of the database by right-clicking the License Server, and choosing Review the Configuration.

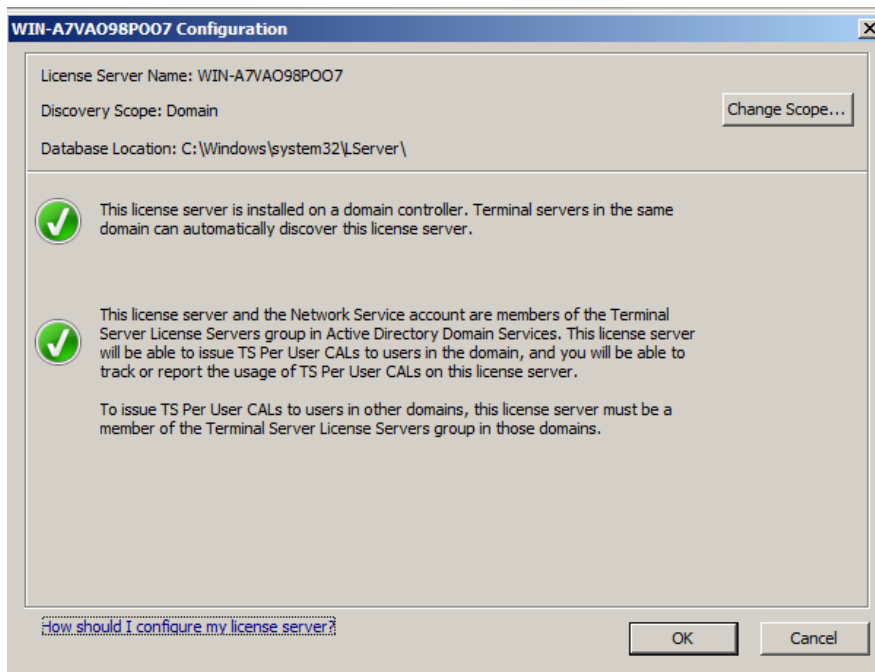


Figure 57: TS LicenseServer

There are typically 2 scenarios when recovering, and details are below:

- You are recovering to the same computer – when you restore the system state and database, you will have both issued and unissued licenses available for use.
- You are recovering to a different computer – you will not have unissued licenses available and must contact the Microsoft Clearing house for recovery. Issued licenses will still be available.

## Configure Terminal Services client connections

### Connecting local devices and resources to a session

Remote Desktop allows users to access local drives and resources in their remote sessions, and is called redirection. Users can access printers, drives, Plug and Play devices, audio, LPT/COM and the clipboard. Server 2008 has enhanced redirection support, and has added media device expansions to support picture and media devices.

This can be configured on the Local Resources tab within the Remote Desktop client.

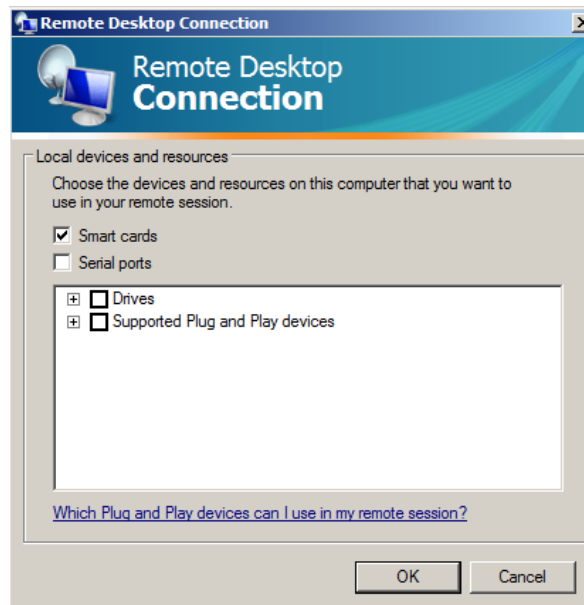
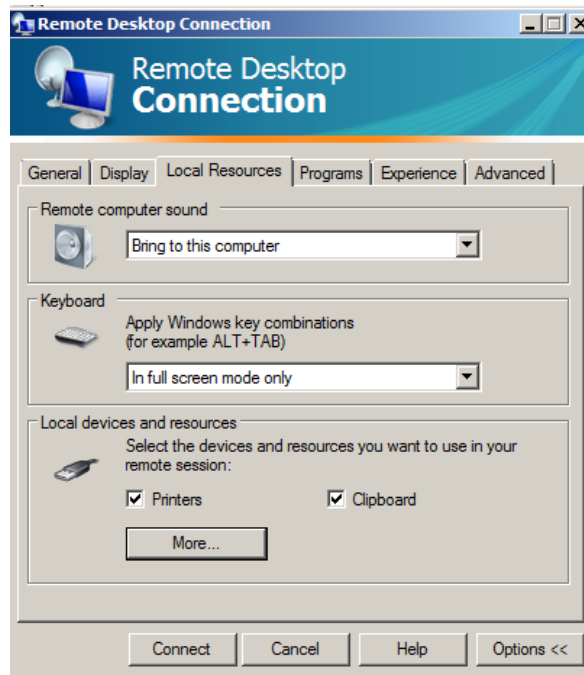


Figure 58: Remote Desktop Connection

## MSTSC and the Remote Desktop Client

At the client level, mstsc.exe is the client application. There are several settings at the client that can be controlled through Group Policy, or be manually configured to customize the session:

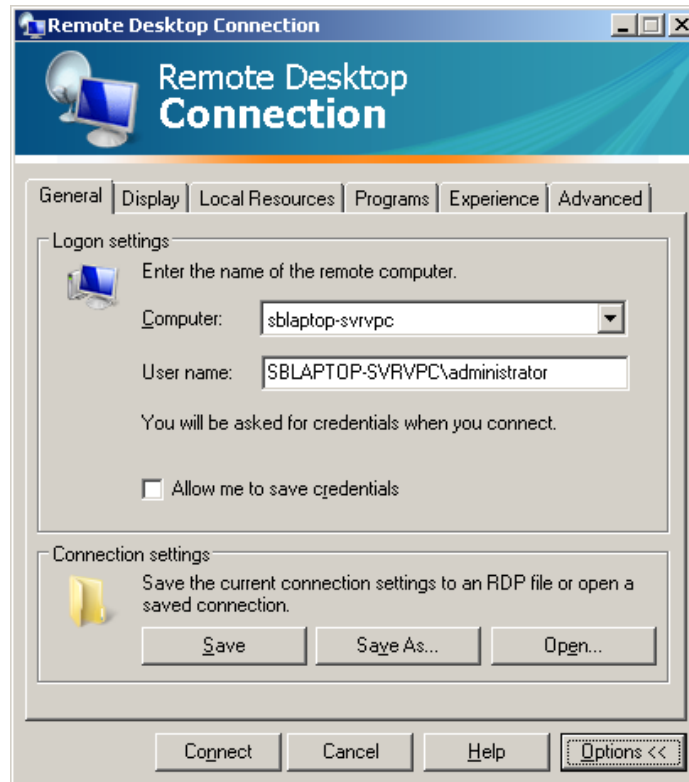


Figure 59: Remote Desktop Connection

The following are the tabs and the configuration items they contain on the RDP interface:

- **General** – provides the basic logon settings, including computer and username to utilize, as well as where to save connections.
- **Display** – Controls the size of the remote desktop, as well as color settings, and whether to connect in full screen mode.
- **Local Resources** – defines sound, keyboard and other local resources behave during remote connections.
- **Programs** – allow you to define programs to start upon successful connections, and set environment folders.
- **Experience** – this tab is key to controlling performance of TS over differing connection speeds. You can set the connection speed, as well as display control and graphics caching.
- **Advanced** – security level warnings, as well as TS Gateway designation and behavior settings.

## Terminal Services Profiles and Home Directories

Terminal Services profiles are created the first time a user logs on by default. In large environments, this can cause issues as the profiles can grow in size over time, and utilize large amounts of disk space. It is recommended that administrators place quotas on TS Users through the file system resource manager to stop the unwieldy growth of profiles. A second option is to create Terminal Services roaming profiles that will allow users to roam, and utilize the profile from wherever they attach. Profiles allows the designation of a TS Home directory for users, and allow for centralized management of user files and information. Below are configuration settings for setting up profiles with home folders:

1. Configure an SMB share on a file server to store the roaming profiles for TS users.
2. Setup an RD Session Host roaming profile path user group policy:

### **Computer Configuration - \Administrative Templates \Windows Components\ Remote Desktop Services \Remote Desktop Session Host\ Profiles \Set path for Remote Desktop Services Roaming Profiles**

3. Limit the cache size through the same key above, but setting Limit the size of the entire roaming user profile cache.
4. Configure Folder Redirection for users with group policy as well:

### **User configuration \Administrative Templates \System \User Profiles \Network directories to sync at Logon/Logoff**

## Single Sign On

Server 2008 provides single sign on capability for terminal services users, and provides ease of administration if you are deploying Line of Business Application or you are centralizing your applications deployment (using term services). This service provides a single credential entry for users, and does not keep prompting them for the same information when they hop from one application to another. To allow for this to occur:

1. On the Windows Vista/7-based device, open the Local Group Policy Editor. Type gpedit.msc and then press ENTER in the Run box.
2. In the left pane, click on the following nodes: Computer Configuration, Administrative Templates, System, and then click Credentials Delegation.
3. Double-click Allow Delegating Default Credentials.
4. In the Properties dialog box, on the Setting tab, click Enabled, and then click Show, and then add your servers to the list.
5. In the Add Item dialog box, in the Enter the item to be added box, type the prefix termsrv/ followed by the name of the terminal server; for example, termsrv/MyServer, and then click OK.

## Configure Terminal Services server options

The majority of the client configuration can be accomplished through the Terminal Services Configuration snap-in. To edit connection settings for RDP, right-click the RDP-Tcp connection listed in the Connections section of the management interface, and choose Properties:

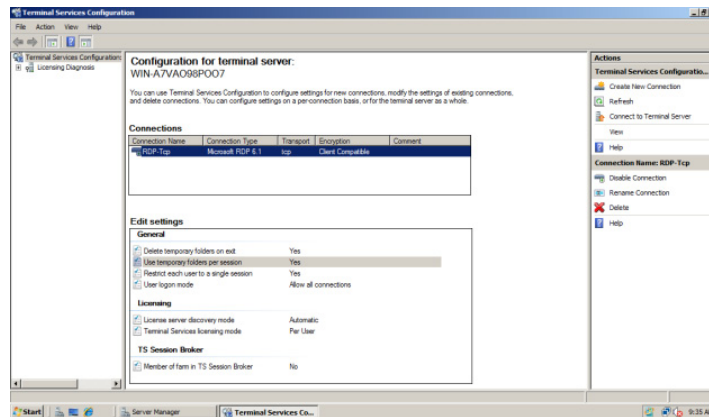
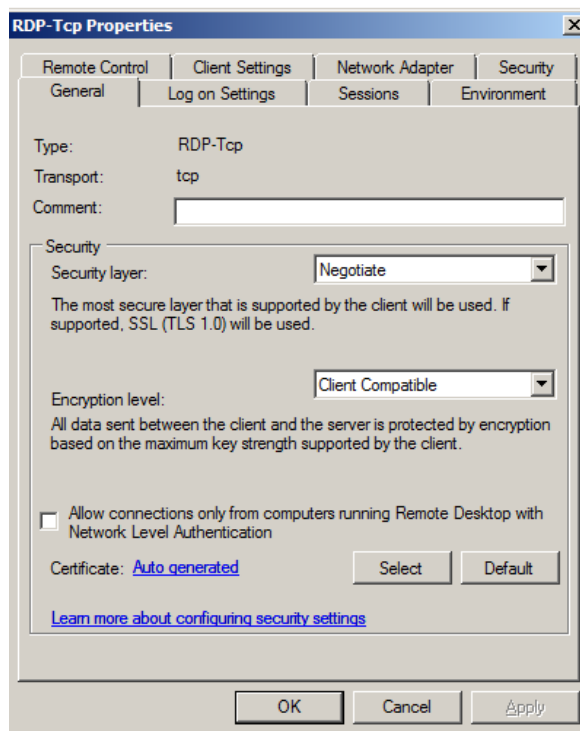


Figure 60: Terminal Service Server Options

The Properties sheet for the RDP-Tcp connection has the following tabs:

- **General** – Allows you to set the Security configuration for client connections.
  - **Security layer choices** – SSL, Negotiate and RDP Security.
  - **Encryption Level** – client compatibility, High or FIPS.
  - **Allowing connections from NLA Clients only.**
  - **Certificate Selection.**
- **Logon Settings** – set whether the client can provide credentials, or set the specific account. Also allows you to always prompt for passwords.
- **Sessions** – provides settings for timeouts and reconnections, including – active session limits, idle session limits, when to end sessions, and how to end a session when limits are reached.
- **Environment** – initial program settings to specify initial programs launched.
- **Remote Control** – whether or not remote control can be accomplished, and if user permission is required.
- **Client Settings** – you can set client color depth, and disable redirection for: drives, printers, LPT/COM, clipboard, audio, etc.
- **Network adapter** – you can choose the network adapter to utilize with the specified protocol, and set connection limits.
- **Security** – specify the users/groups that can connect to terminal server.



**Figure 61:** RDP-TCP Properties

On the configuration page, there are the most frequently accessed settings provided on the interface, and you can double-click any of them to set.

Under the edit settings section, you will also have access to Licensing and Session Broker settings, which open the following Properties interface:

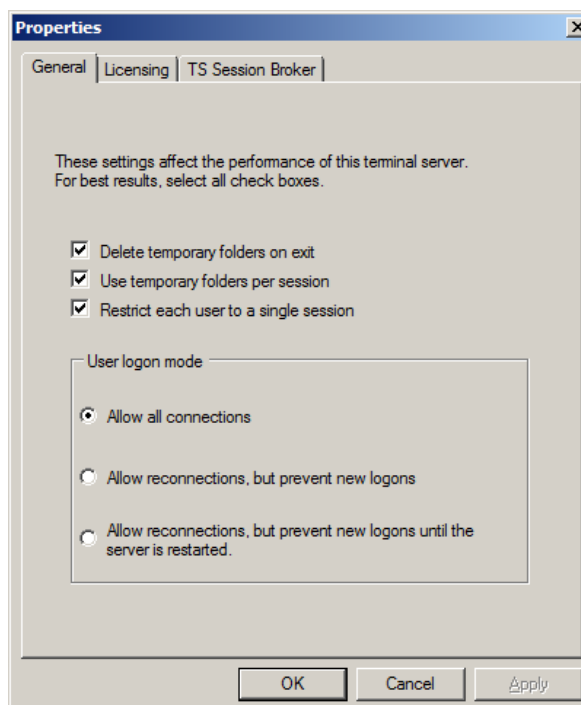


Figure 62: Properties

The tabs on the interface are the following:

- **General** – folder settings on temp folders, ability to restrict users to a single session. Also, the user logon mode where you can allow all connections, allow reconnections but prevent new logons, and allow reconnections, but prevent new ones until a server restart (used for server maintenance).
- **Licensing** – this is where you can set per device or per user licensing. It also allows you to set auto discovery of license servers, or specify a license server.
- **TS Session Broker** – all settings for participation in a session broker TS farm. Including load balancing and IP settings.

Terminal Server settings can be controlled through the use of Group Policy, and settings can be placed in the Computer Configuration or User Configuration/Administrative Templates/Windows Components/ Terminal Services. Within this container, you have the ability to control Remote Desktop Settings, TS Licensing, and Generic Terminal Services Properties. Below is an overview of the tree:

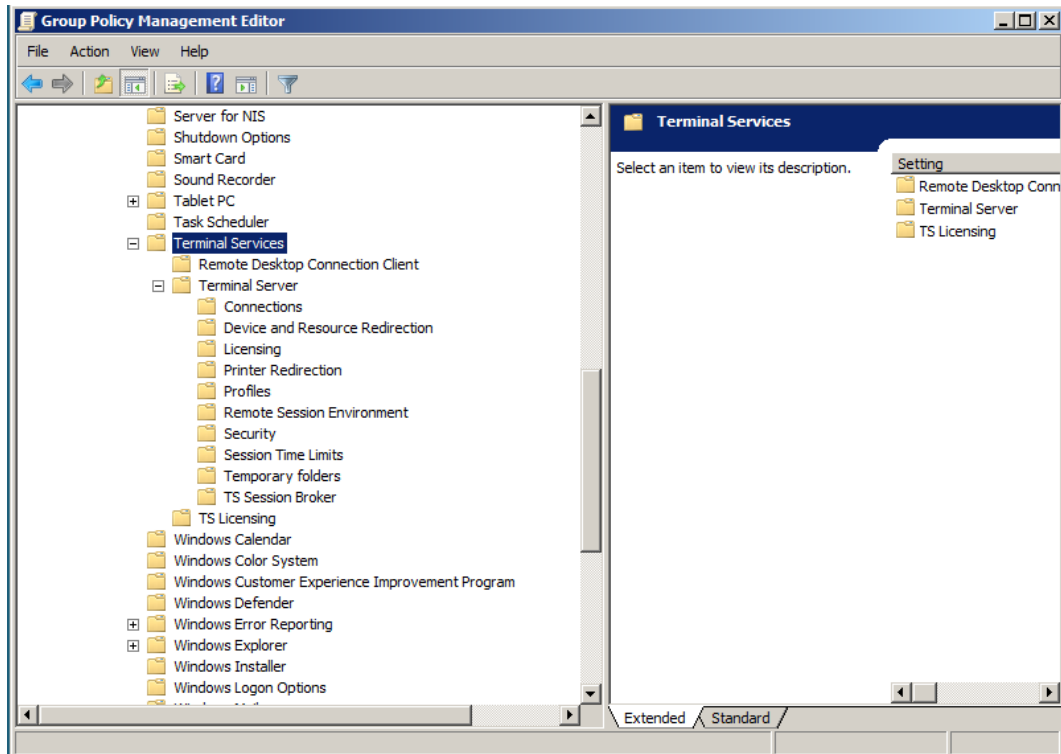


Figure 63: Group Policy Management Editor

## Terminal Services Is Renamed in Windows Server 2008 R2

One of the most important changes to Terminal Services for candidates taking the 70-649 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)

Figure 64: Terminal Services Renamed



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

**Figure 65:** Role Services Renamed

For the purposes of the exam, knowing the 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>. New features that should be considered include:

- **Per-user RemoteApp filtering:** Using per-user RemoteApp filtering, you can filter or limit the list of RemoteApp programs shown to a user account when logged on to the RD Web Access Server. All RemoteApp programs were shown to users prior to the release of Windows Server 2008 R2.
- **Fair share CPU scheduling:** This feature provides an even distribution of processor time across RDS sessions using dynamic loads. It is controlled in the registry location at: HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\SessionManager\DFSS\EnabledDFSS. When this value is set to 1, the fair share CPU scheduling is enabled. When set to 0, it is disabled.
- **Windows Installer RDS compatibility:** Previous versions of RDS required that administrators pre-install applications that required per user configurations because only one Windows Installer installation could be performed at a time. The Windows Installer RDS compatibility features allows for the queuing of these installation requests and processes them one at a time to avoid conflicts.

## Configuring a Web Services Infrastructure Overview

Server 2008 incorporates Internet Information Service 7, which has some expansive new features over its predecessor. Overall features/enhancements include:

- **Enhanced extensibility model** – core server API provides the ability to develop modules in core code languages (C/C++) and managed code, including C#.
- **Powerful troubleshooting and diagnostic tools** – built in enhanced error reporting and diagnostics allow streamlined troubleshooting.
- **Administrative delegation** – sites and features can be delegated to simplify administration.
- **Enhanced security through modular structure** – the new version includes over 40 segmented modules that compartmentalize operations, and harden security.
- **Configuration simplicity** – addition of web.config configuration files provides simple copy/xcopy features to duplicate settings across farms.

- **Application and health management** – provides enhanced monitoring and activation features.
- **Administrative improvements** – all in one application interface provides simple yet granular configuration.

#### IIS Server Core Features:

- **Configuration Validation** – automatically validates server applications and configurations and reports errors or misconfigurations.
- **Anonymous Authentication** – this is the default authentication method.
- **HTTP Cache** – IIS & supports Kernel mode caching, and will store content with a cache to improve performance.
- **Protocol Support** – the HTTP protocol (HTTP 1.1) have numerous items that are supported through any web server. Most importantly are redirection, custom headers and keep alives.

#### Common HTTP Features:

- **Directory Browsing** – if no default document is specified and browsing is enabled, and then requests to the site will present a listing of all the content within the directory.
- **Default Document** – this is a default page that will be displayed when there is no direct page specified in the request. You can configure the default document name.
- **HTTP Errors** – IIS7 supports custom and standard errors.
- **Static Content** – support for html fixed content and images.
- **HTTP Redirection** – this feature is not enabled by default, but can be selected. This is typically used to redirect requests from an old site or content location to a new one.

#### Monitoring and Diagnostic Features:

- **Standard Web Server Logging** – logging is enabled by default, and gives the administrator the capability to select the fields. Default logs files location is in the system root, under inetpub\logs\logfiles. By default these are text-based files.
- **Custom Logging and ODBC logging** – the system now allows the ability to customize logging and also log into an ODBC data source.
- **Tracing** – This feature provides the ability to track failed web requests, and further isolate application or server issues.

## Configure Web applications

The Application Server Role is new to the Windows Server operating system and is a primary feature of Server 2008. It provides an integrated environment for running custom built web and web service applications, and can service users or other server making app requests. Typically they will take advantage of several of the key components within the application server:

- Internet Information Services (IIS) 7
- .NET Framework versions 3.0 and 2.0
- ASP.NET
- COM+
- Message Queuing
- Web services - built with Windows Communication Foundation (WCF)

The Application Server role is available in:

- Windows Server 2008 Standard
- Windows Server 2008 Enterprise
- Windows Server 2008 Datacenter
- Windows Server 2008 – Itanium

NOTE: You **cannot** add the application server role on Web Server 2008.

When installing the Application Server Role, you can add the following options:

- **Web Server** – this installs IIS, and provides web services, asp.net support and WCF.
- **COM+ Network Access** - for remote calling of applications that are built on and hosted within COM+ and Enterprise Services components. COM+ Network Access is one capabilities of Windows Server 2008. Newer applications may use WCF.
- **Windows Process Activation Services (WAS)** - WAS can start and stop applications dynamically based on messages that are received over the network using Hypertext Transfer Protocol (HTTP), TCP, Message Queuing, and Named Pipes.
- **TCP Port Sharing** – Allows multiple applications to share a single port for inbound communication and messaging.
- **Distributed Transactions** – can be used to coordinate transaction processing over the network.

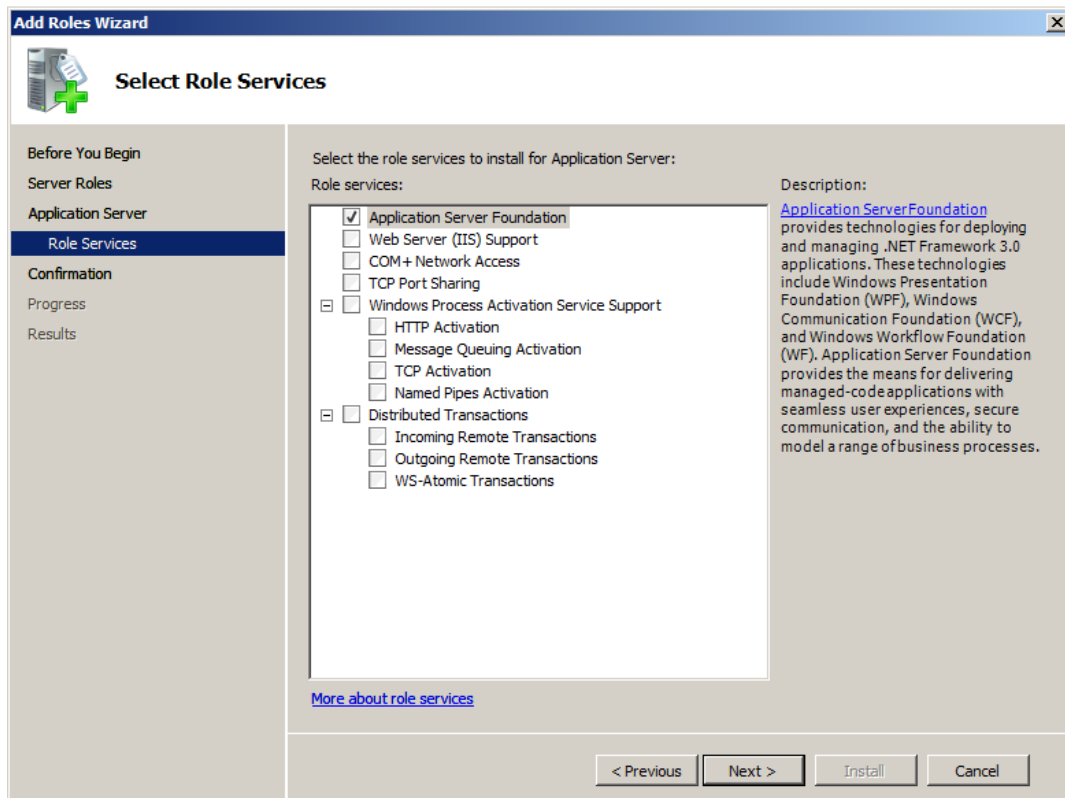


Figure 66: Select Role Services

Application services are managed through the Application Server snap-in. Within this management interface, you can view all the component services, and configure specific properties for DTC and Component Services.

## Creating Web Applications

To create a web application, you need to open the IIS Manager, and expand the server node, and then the Sites node. Right-click the Default Web Site node, and choose Add Application. In the Add Application dialog box, you will be prompted for an Alias, as well as the physical path to the new application. This location should be unique and not house any other applications. You can then choose the application pool to utilize, as well as set pass through authentication options.

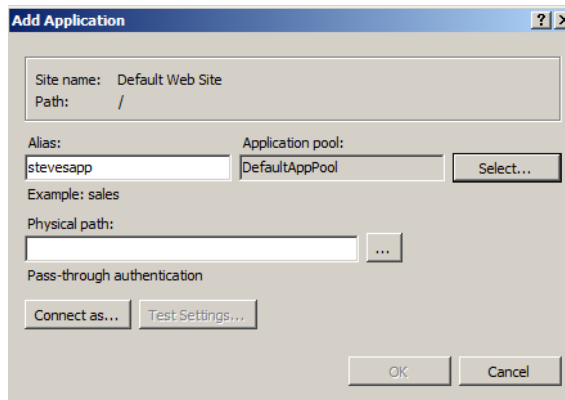


Figure 67: Add Application

## Application Pools

Application pools in Server 2008 provide the ability to overcome a major weakness in IIS in the past: applications easily affected other applications. Leaks and bugs caused the entire IIS server to crash or have performance issues in the past. Application pools provide application isolation, and prevent runaway apps from impacting other applications on the same server through compartmentalization of the application process. There are default app pools, and they include Classic .Net and Default. To create and configure a new application pool you right-click the Application Pools node, and click Add Application Pool. You will be prompted to name the pool and choose the .Net framework to utilize. Once this is established you can then configure the application.

To configure advanced settings, right-click the created application. This provides granular control over how the applications runs, the resources utilized and many other details below:

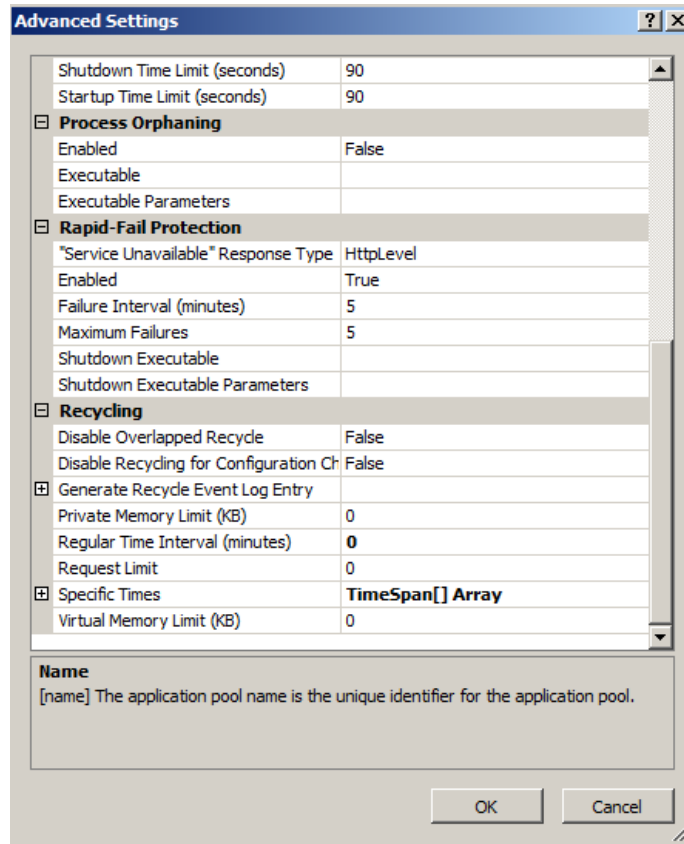


Figure 68: Advanced Settings

Application Pools within IIS 7 are groups of one or more URLs that are served by a worker process or a set of worker processes. They are set boundaries or containers for applications which keep them confined so as not to affect other applications.

Application pools offer the following benefits:

- Overall performance improvement for applications. You can place resource intensive applications within their own pool to ensure they do not affect other applications on the server.
- Improved application availability. The application pools provide segmentation so that the failure of one application will not fail others, nor bog down the web server.
- Improved security. When you isolate applications, you prevent unauthorized access to penetrate other application because they are running within their own security context and boundary.

Application pools in IIS7 run in two modes:

- **Integrated mode** - The application pool mode affects how the server processes requests for managed code. If a managed application runs in an application pool with integrated mode, the server will use the integrated, request-processing pipelines of IIS and ASP.NET to process the request.
- **Classic mode** - If a managed application runs in an application pool with classic mode, requests are managed as they were in IIS 6, and the server will continue to route requests for managed code through Aspnet\_isapi.dll.

Creating an application pool is simple, and is accomplished through the use of the IIS Management Snap-in. Select Application Pools, and right-click, select Add Application Pool. Name the pool, select the .Net framework you require, and choose the pipeline mode of either classic and integrated. Once you have created the pool, you can now set advanced properties, and control settings through several sections:

- **General** – provides the ability to change the .Net framework, and Pipeline Mode, as well as the queue length.
- **CPU** – You can set processor specific items for the application pool, including affinity and interval minutes.
- **Process Model** – provides the ability to set timeouts, and max worker processes, as well as time limits.
- **Rapid-fail Protection** - allows control of how services are shutdown and failure intervals.

#### Microsoft .Net and ASP

The .Net framework is an overall solutions framework that provides ease of development for applications, and a virtual machine that manages program execution. The .Net Framework has several components that include:

- **Windows Communication Foundation** – this is a messaging system that allows communications between services.
- **Windows Presentation Foundation** – This is an integrated interface system and graphics engine based on XML.
- **Windows Workflow Foundation** – provides workflow task automation and options.
- **Windows CardSpace** – a secure identity management system.

The portion of this framework that provides Web application development technology is ASP.NET. There are several configuration options for .Net, but most are configured with the application itself. Importance lies on proper application pool configuration, and the setting of trust levels. .Net trust levels specify a built-in security configuration for different applications. You can set the trust level to a number of levels, to protect servers from code that has been compromised.

## Manage Web sites

### Migrating and Upgrading to IIS 7

There are two ways to move Web Sites and Applications to IIS 7: upgrading and migrating.

When upgrading/migrating, there are several point of focus:

- **Hardware Compatibility** – You must ensure that the current hardware will meet Server 2008 and IIS 7 minimums.
- **Application Considerations** – Most applications will require some code upgrades to ensure compatibility. Microsoft provides a free tool called the Web Platform Installer that can help in the transition process.
- **Move to Request Filtering** – URLScan has been replaced by a core function in IIS 7 called request filtering.
- **ASP.NET** – You will need to ensure proper script mapping in your application pools.
- **WebDav** – This is not included in IIS 7 by default, but can be downloaded from MS.

## Configuring Sites and Virtual Directories

All website configuration and administration can be accomplished through the use of the IIS snap-in.

To add a website, you select the Sites node in the tree, and right-click, select Add Website. Below is the presented dialog:

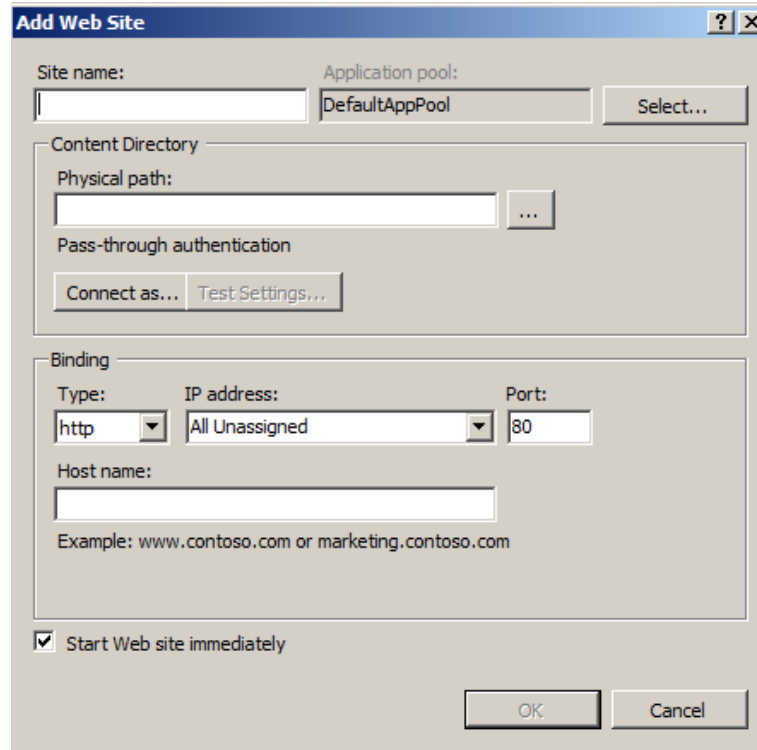


Figure 69: Add Web Site

1. Enter the site name. This will be the display name within the administrative interface.
2. IIS 7 allows you to select the application pool in which to run the site. The default app pool utilize .Net 2.0. If your site requires specific .Net versions, you can select it here.
3. The Physical path is the location of the web site or application files. Ensure proper security is set on these site directories and files.
4. You can configure either a specific user, or a configured application user for the site.
5. Designate whether the site is HTTP or HTTPS, assign the IP and Port, and then specify the host name that clients will utilize to access the site (This is required for host header functionality where multiple hostnames are assigned to one IP).

Once a site has been established, you can set specific additional settings by right-clicking the site:

- **Edit permissions** – provides the ability to set NTFS permissions on the site folder and files.
- **Add Application** – allows the creation of web application roots within the site and the ability to specify aliases and permissions.
- **Add Virtual Directory** – allows you to create virtual web directories off the parent site.
- **Edit bindings** – provides the ability to add additional bindings to the site, including protocols, ports, IPs, and hostnames.

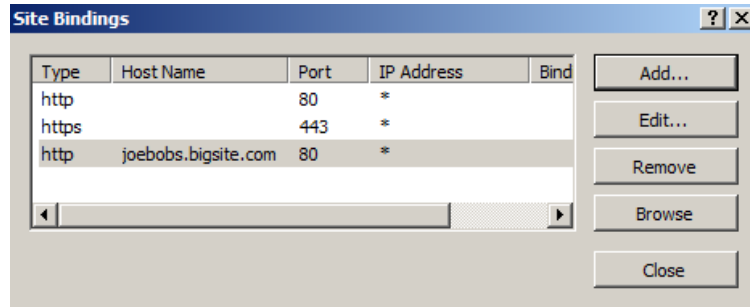


Figure 70: Site Bindings

- **Manage Web Site** – allows you to Start, Stop, Restart, Browse and access Advanced Settings.
- **Manage Web Site - Advanced Settings** – provides a full set of advanced settings for the site, including credentials, logon types, connection limits and tracing.

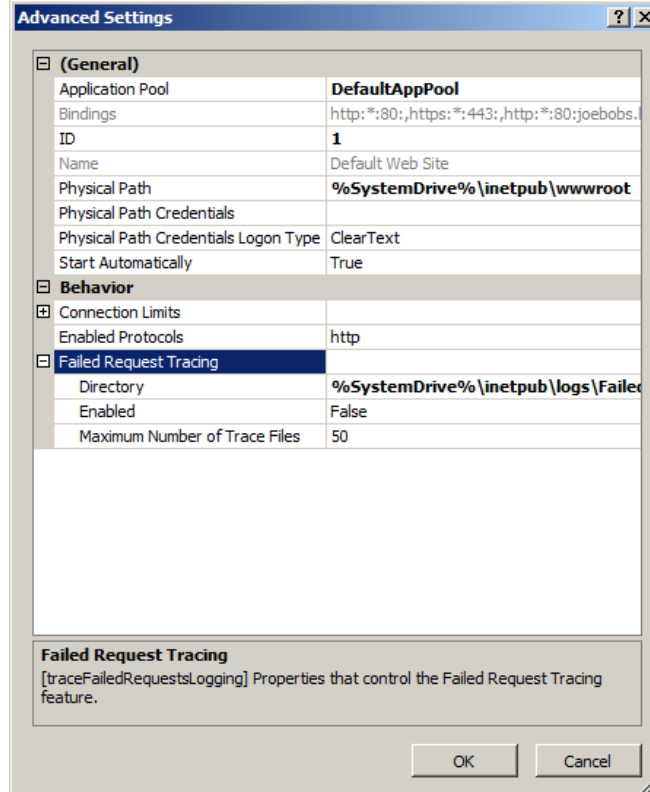


Figure 71: Advanced Settings



Migrating Web Applications and/or sites can be a tricky operation, and Microsoft provides the Web Deployment tool to assist in the migration operation.

For more information you can accomplish with the tool:

- Migrate up to 1,000 web sites from IIS6 to IIS7 including all the configuration settings, certificates and content.
- Migrate a single web application.
- Migrate an entire server (all web sites, app pools, etc.) and all its settings from IIS6 to IIS7.
- Migrate a custom group comprised of sites, app pools, assemblies, COM objects, registry keys, content and more from IIS6 to IIS7.

The tool process can be summarized below:

1. Examine your current site dependencies using the following command:  
`msdeploy -verb:getDependencies -source:metakey=lm/w3svc/1`

Make sure you can recreate these on the target.

2. Configure the target server, and ensure all dependencies are satisfied.
3. Migrate using the following command sequence:

On the source Server: `msdeploy -verb:sync -source:metakey=lm/w3svc/1 -dest:archivedir=c:\site1archive > msdeployarchive.log`

On the Dest Server: `msdeploy -verb:sync -source:archivedir=c:\site1archive -dest:metakey=lm/w3svc/1 > msdeploysync.log`

## Configure a File Transfer Protocol (FTP) server

Server 2008 has some changes within the FTP publishing service:

- **Support for recent internet standards** – IIS 7 help manage secure publishing of content by using FTP over SSL, or FTPS. It also supports IPv6 and UTF 8.
- **Simplified Administration** – Provides the ability to enable FTP services for an existing web site so you do not have to create and manage two separate entities. IIS7 also provides support for multiple sites assigned to a single IP through the use of hostnames.
- **Improved Security** – Enhanced logging and auditing functions, along with authentication through IIS manager provides the ability to control and monitor access.

Creating FTP sites is simple and is accomplished through the IIS Manager, by right-clicking and selecting New. Once you create a site, you can right-click and edit specific properties through the tabs:

- **FTP Site** – set assigned IP, port, connection limits and logging. You can also check existing connections through this tab.
- **Security Accounts** – you can set anonymous connections and provide an account.
- **Messages** – provides the ability to set Banner, Welcome, Exit and Max Connection messages.
- **Home Directory** – set the directory location for FTP files, as well as give users FTP Read, Write and set logging.
- **Directory Security** – allows rules for access set by IP or Network.

External sites should be configured to utilize SSL as FTP passes usernames and passwords in clear text.

## Configure Simple Mail Transfer Protocol Services (SMTP)

Windows Server 2008 SMTP Server conforms with the Internet-standard Simple Mail Transfer Protocol (SMTP) to deliver and transport messages based on specifications in Request for Comments (RFC) 2821 and RFC 2822. It also provides enhancements that expand the basic delivery functions of the protocol. There are options that provide the ability to control the routing and delivery of messages, and can provide secure communications.

Simple Mail Transfer Protocol (SMTP) can be installed as a feature through Server Manager, and provides the ability to relay and receive email. To manage the service, you need to utilize the IIS 6 manager, and to manage your virtual server, right-click and choose properties. Below are the tabs:

- **General** – You can choose the IP to utilize, limit connections, set timeouts and enable logging.
- **Access** – The following can be set through this interface.
  - **Access control** – set the authentication method as anonymous, basic or integrated.
  - **Secure communication** – allows you to require TLS.
  - **Connection Control** – provides restrictions on IP, Network or domain names.
  - **Relay Restrictions** – provide a listing of computers allowed to relay mail through the host. By default, relaying is not allowed.
- **Messages** – set message limits: size, session size, number, recipients. Also, set badmail directory.
- **Delivery** – set a number of delivery parameters, including:
  - **Outbound** – set retry intervals, delay notifications, and expiration timeouts.
  - **Local** – set delay and expiration timeouts.
  - **Outbound Security** – set authentication requirements for outbound connections – anonymous, basic, integrated and TLS.
  - **Outbound Connections** – set connection limits, retry limits and port number.
  - **Advanced** – set max hop count, masquerade domain, FQDN and smarthost. Also allows you to set reverse DNS lookup on incoming messages.
- **LDAP Routing** – integrates with LDAP to resolve senders and recipients.
- **Security** – allows the designation of operators of the service.

As sub-configuration of the SMTP Virtual Server (Several virtuals can be run within a single server instance, just on separate ports), you can also configure domains for which you will handle mail. Once configured, you have the ability to configure specific properties for domains:

- **General** – configure allowing mail to be relayed for a domain, outbound security and specific DNS routes or SmartHosts.
- **Advanced** – provides support for ATRN queuing.

SMTP Smart hosts are mail relays that provide authentication and routing services as an intermediary prior to the final mail destination.

## Manage Internet Information Services (IIS)

IIS administration has been extended in version 7 through the addition of Appcmd.exe. This utility can be used to configure and query objects on your Web server, and to return output in text or XML. The following are examples of tasks that you can perform with Appcmd.exe:

- Stop and start sites.
- Create and configure applications, sites, application pools, and virtual directories.
- Start, stop, and recycle application pools.
- View information about requests and worker processes.

Before you execute a command with this utility, you must change directories or use the full path in the command line or batch file. The utility resides within System Root\system32\inetsrv\.

Below is a summary of options for the command for the command:  
 APPCMD (command) (object-type) <identifier> </parameter1:value1 ...>

Supported object types:

- **SITE**- Administration of virtual sites
- **APP**- Administration of applications
- **VDIR**- Administration of virtual directories
- **APPPPOOL**- Administration of application pools
- **CONFIG**- Administration of general configuration sections
- **WP**- Administration of worker processes
- **REQUEST**- Administration of HTTP requests
- **MODULE**- Administration of server modules
- **BACKUP**- Administration of server configuration backups
- **TRACE**- Working with failed request trace logs

General parameters:

- **/?** Display context-sensitive help message.
- **/text<:value>** Generate output in text format (default).
- **/xml** Generate output in XML format. Use this to produce output that can be sent to another command running in /in mode.
- **/in or -** Read and operate on XML input from standard input. Use this to operate on input produced by another command running in /xml mode.
- **/config<:\*>** Show configuration for displayed objects.
- **/metadata** Show configuration metadata when displaying configuration.
- **/commit** Set config path where configuration changes are saved. Can specify either a specific configuration path, "site," "app," "parent," or "url" to save to the appropriate portion of the path being edited by the command, "apphost," "webroot," or "machine" for the corresponding configuration level.
- **/debug** Show debugging information for command execution.

The `appcmd` can be utilized to backup and restore configurations of the web server by specifying the following:

*Appcmd add backup MyIISBackup*

MyIISBackup is a name you can specify to manage your backup once it is created. Once you have created backups, they can be listed by the command:

*Appcmd list backups*

To restore a backup, utilize:

*Appcmd restore backup MyIISBackup*

The IIS Management interface has been enhanced and extended, and can be very confusing upon first glance. The interface allows you to group by area or category, depending on your preference. At the server level, there are several icons within the Management Area:

- Feature Delegation – this will list all of the features that can be delegated within a site. The delegation state of a feature will determine whether non-administrative users who have permissions to a site or application can configure the feature within that site or application.

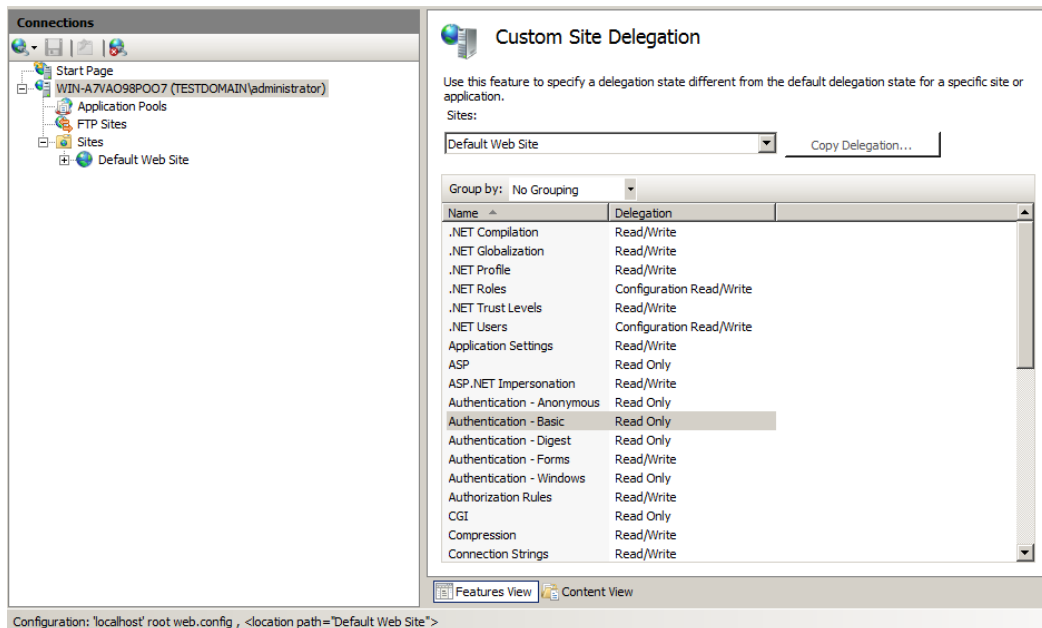


Figure 72: Custom Site Delegation

- IIS Manager Permissions and IIS Manager Users – both allow you to designate users that can manage, and their permission levels.
- Management Service – provides the ability to set requirements and restrictions on how remote managers will connect to the server to manage IIS.
- Share Configuration – provides the ability to designate a shared configuration location.

## Configure SSL security

In order to enable Secure Sockets layer you must first configure a server certificate, and then create an HTTPS binding to enable SSL. SSL can be enabled at 4 levels:

- Site
- Application
- Physical Directories
- Files/URLs

There are several reasons to require a secure connection to your web server:

- When you have confidential or personal content on your server, and it must be protected by encrypted communications.
- When it is required for users to confirm the identity of the server before they transmit confidential information.
- When client certificates to authenticate clients that access your server are required.

To require SSL, open IIS Manager, and Select the site, app or directory to secure. Double click the SSL Settings, and select require SSL, as shown below:

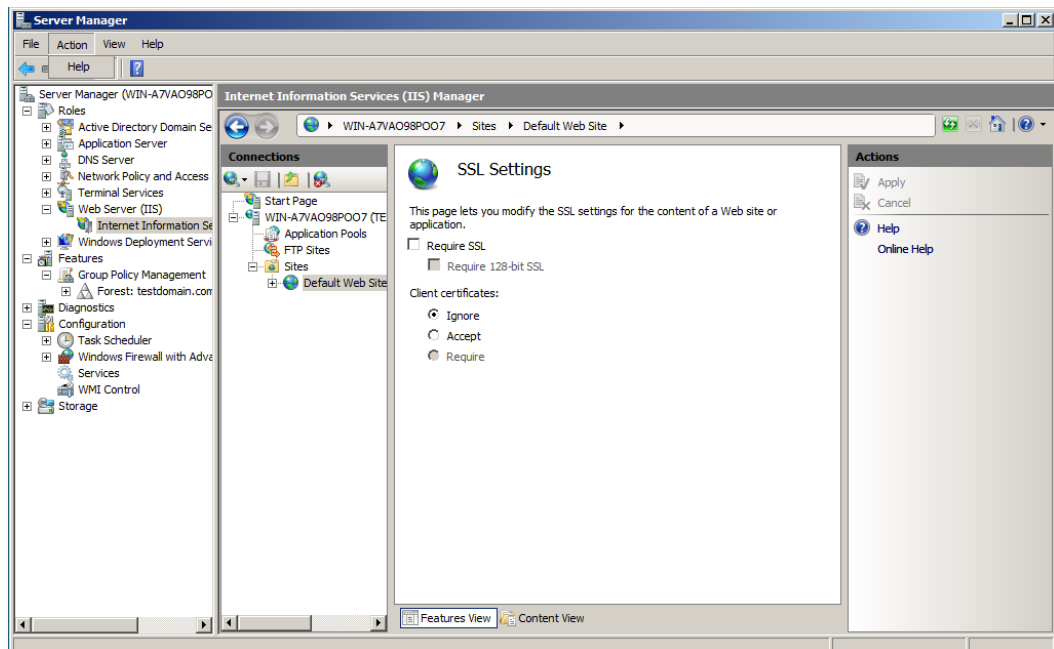
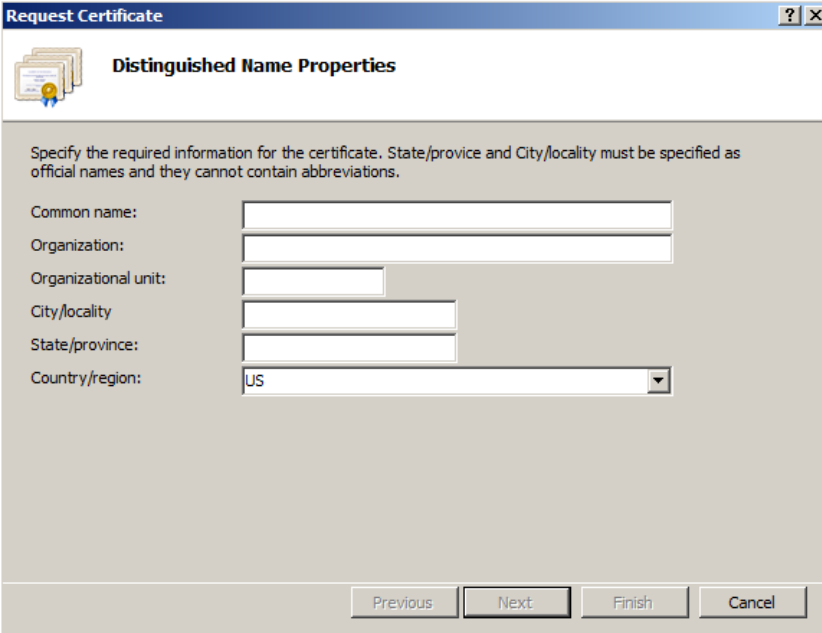


Figure 73: Server Manager

You can also require 128 bit encryption, and setup Client Certificate handling.

In order to enable SSL, you must first request a certificate, and then install it on the server. The certificate request is created through the following procedure:

1. Open IIS Manager, and highlight the server.
2. In the Features View, double-click Server Certificates.
3. In the Action pane, click on Create Certificate Request.



The screenshot shows a Windows dialog box titled "Request Certificate" with a sub-header "Distinguished Name Properties". Below the sub-header is a small icon of a certificate. The main text reads: "Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations." There are six input fields: "Common name:", "Organization:", "Organizational unit:", "City/locality", "State/province:", and "Country/region:". The "Country/region" field is a dropdown menu with "US" selected. At the bottom of the dialog are four buttons: "Previous", "Next", "Finish", and "Cancel".

**Figure 74:** Request Certificate

4. You will be prompted to fill out information on your organization.
5. Continue the wizard and select the defaults. Once completed, a certificate request file will be created, and you will need to forward this to a Certificate Authority like VeriSign.

Once you receive the certificate request back, you will need to load the received certificate and bind it:

1. Open Server Certificates and in the Action pane, click Complete Certificate Request. Type in a Name for the certificate and it will load into the system.
2. Right-click the site node, and select Edit Bindings. You will now have to edit the 443 binding, and choose the certificate to bind to that port. Once this is done, communications over SSL will be enabled.

## Configure Web site authentication and permissions

IIS 7 provides for several methods of authentication:

- **Anonymous** – this is the default authentication method, and requires no credentials to view web content. The web service utilizes the IUSR account to access content and NTFS file stores.
- **Forms Authentication** – this method redirects users to an HTTP form to collect and transmit logon information. By default, forms information is transmitted in clear text, so it is recommended to enable SSI on all forms authentications.
- **Challenge-based Authentication** – this method sends a HTTP 401 message to prompt the user for logon credentials. IIS supports the following challenge methods:
  - ▶ **Basic Authentication** – supported by all browsers, and passes information in clear text by default.
  - ▶ **Digest Authentication** – uses the HTTP 1.1 standard to provide a secure method of transmitting credentials, and authenticates to a domain controller.
  - ▶ **Windows Authentication** – uses NTLM or Kerberos to validate credentials against a Windows based system. Mostly used in intranets where domain controllers can be contacted.
- **ASP.NET Impersonation** - ASP.NET impersonation can be utilized when you want to run your ASP.NET application under a different security context from the default security context for ASP.NET application. When you enable impersonation for an ASP.NET application, the application can run in two different contexts: either as the user authenticated by IIS 7 or as an arbitrary account that you set up. By default, ASP.NET impersonation is disabled.
- **Client Certificates** – this method is used to validate the users identity, and has 3 main modes of operation:
  - ▶ **One to one mapping** – every client computer certificate is held by the server, and is checked upon access.
  - ▶ **Many to one mapping** – the server checks that the certificate contains specific information such as subject or organization. This method is utilized in high user count environments, where storing all the client certs is not practical.
  - ▶ **Active Directory Mapping** – AD Certificate Services provides certificate mapping. Organization must have its own CA.

Below is the required modules for each authentication type.

Method	Module
Anonymous	AnononymousAuthModule
ASP.NET impersonation	Managed Engine
Basic	BasicAuthModule and TokenCacheModule
Client Certificates	iisClientCertificateMappingModule
Active Directory Cert Mapping	CertificateMappingAuthenticationModule
Digest	DigestAuthModule
Forms	FormsAuthenticationModule
Windows	WindowsAuthenticationModule

**Figure 74:** Authentication Types

The authentication method is configured in IIS Manager through the Authentication Icon. Double-clicking provides you with a dialog that provides the ability to enable/disable authentication methods, and right-clicking the method will let you edit specific method properties.

Security and Permissions in IIS are controlled through several items in the Features View Security Category:

- **Authorization Rules** – provide the ability to restrict specific users and roles to specific content and applications. Below is the rule creation dialog:

**Figure 75:** Authorization Rules



- **.Net Roles** - .NET Roles offer the ability to categorize a set of users and perform security-related operations, such as authorization, on a defined set of users.
- **.Net Trust Levels** – permits the setting of levels of trust for .Net applications. Each level has all the features of those above them:
  - ▶ **Full** – app has all the permissions of the user account running it.
  - ▶ **High** – app cannot call unmanaged code, call serviced components, access message queuing, call ODBC.
  - ▶ **Medium** – cannot access outside of application directory or make network or web service calls.
  - ▶ **Low** – cannot write to the file system or run any application test functions.
  - ▶ **Minimal** – totally limited to calculations.
- **.Net users** – provides the ability to specify users for .Net activities.
- **Authentication** – sets the authentication method.
- **IPv4 Addresses and Domains** – control who can access content based on their source addresses/domains.

## Web Services in Windows Server 2008 R2

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 sever 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-pssnapin WebAdministration command. Once installed, it provides more than fifty cmdlets documented here <http://technet.microsoft.com/en-us/library/ee790599.aspx>.
- **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.

## Practice Questions

### Chapter 1

1. Johnson is the systems administrator for Taggart & Sons, a large law firm in Miami. Johnson is in the process of upgrading his company's servers from Windows Server 2003 to Windows Server 2008. Johnson wants to deploy RODC's in the law firm's branch offices since they do NOT have any IT personnel at those remote offices. All the branch offices are currently in the same domain as the home office. Johnson upgrades his first server, a Windows Server 2003 DC, at the home office to Windows Server 2008 Enterprise. Johnson logs onto his workstation computer as an Enterprise Admin and tries to run the `adprep /rodcrep` command from the infrastructure master through a command prompt, but he receives an error. What MUST Johnson do before he can successfully run this command? Select the best answer.
  - A. He must raise the forest functional level to Windows Server 2003.
  - B. He must log on to a computer in the domain as a schema admin.
  - C. He must log onto the domain controller that holds the schema master operations role.
  - D. He must enable the Bridge all site links option in the Sites and Services snap-in for the links between the branch and home offices.
  
2. Neil is the senior network administrator for the University of Campbell, a small college in Oregon. Every server on the college's network is using Windows Server 2008 Enterprise. One of the developers in the IT staff has created a web application that allows students to log in and check their grades. These students are given an Active Directory account on the college's network to authenticate them when they login. Campbell has an agreement with another local university allowing them to take classes at Campbell while still being enrolled at the other school. The other school's president would like his students to be able to log into the web application as well, to check grades since they are taking classes at Campbell. Neil definitely does NOT want the students from the other college to have Active Directory accounts in his network, so he sets up Active Directory Federated Services to allow the Active Directory accounts from the other college to have access to the web application. After the initial setup, they find that the server running the Federated Services is being taxed too heavily, so Neil decides to install two more servers with Federated Services. Neil does NOT want to publish three URLs that would have access to the web application; he wants one address that students can navigate to that would choose one server running Federated Services that is currently available. How would Neil accomplish this task of using one name to gain access to any one of the three servers running Federated Services? Select the best answer.
  - A. Neil should install Active Directory Lightweight Directory Service on a server at the perimeter of his network. This would allow the students to have an account on that server and use single-sign-on to access their information.
  - B. To enable one URL to point to any of the three servers, Neil should edit the `default.htm` file on the first web server that was installed. Neil needs to add the IPs of all three web servers to this file.
  - C. Neil should enable static cookies to all three web servers that would help redirect browsers to the appropriate web server.
  - D. Neil should use Microsoft Network Load Balancing to allow one address to point to any of the THREE web servers that is available. Network Load Balancing allows a clustered IP to point to a list of web servers' IPs.

3. Stephanie is the systems administrator for Meley Enterprises, a marketing firm based out of Miami. In an effort to save money on hardware, Stephanie has decided to install Hyper-V on four Windows 2008 Enterprise servers instead of having to purchase four extra servers. All the servers have x64-based processors and run on Intel VT-enabled machines. Stephanie installs Windows Server 2003 SP2 for the guest operating systems on the four servers. After installation, the guest OS will NOT boot and the servers receive an error in the system event log that states: "Hypervisor launch failed at least one of the processors in the system does NOT appear to support the features required by the hypervisor." What action does Stephanie need to take to get the guest operating systems to function properly? Select the best answer.
- A. Stephanie needs to install Windows Server 2008 for the guest operating systems since Server 2003 is not supported.
  - B. Stephanie needs to make sure that the Execute Disable feature is enabled in the BIOS.
  - C. In order for the hypervisor to boot, the Execute Disable feature in the BIOS must be disabled.
  - D. Stephanie needs to enable her PXE compliant NIC to be enabled in the BIOS. This allows the guest OS to boot properly.
4. Kevin is the network administrator for Gearing Up Racing, Inc., a motorcycle manufacturing company in Seattle. Kevin has recently migrated the company's network to a Windows 2008 Active Directory from Windows 2003. Kevin's company also recently purchased 30 laptops for salesmen that will be traveling for the company, trying to create contacts and make clients. Because of all these new mobile users needing access to the network while on the road, Kevin is worried about his network's security. Kevin wants to be able to manage network security policies, and he wants to ensure that all mobile users comply with a certain set of security standards before they are allowed to authenticate on the network. These standards will include: patches, virus definitions, and hardware configurations. What Windows Server 2008 technology would allow Kevin to accomplish what he needs? Select the best answer.
- A. Network Access Protection would allow Kevin to manage security policies and ensure that mobile users have to comply with standards before being allowed onto the network.
  - B. If Kevin used WSUS, he would be able to ensure that all computers had the most recent Microsoft updates before logging on to the network.
  - C. IPSec, built into Windows Server 2008, would allow Kevin to control the mobile computers that log onto his network.
  - D. Active Directory Certificate Server (AD CS) would allow mobile users to be verified before logging onto Kevin's network.
5. You are the network administrator for your company. You oversee the entire network, which consists of one Windows Server 2008 Active Directory domain. You have successfully installed Active Directory Lightweight Directory Services (AD LDS) on one of the domain controllers. This domain controller is at another office than the one you work in. You have opened port 389 on the firewall, so you can connect to the AD LDS instance on the domain controller when you get back to the main office. When you use `ldp.exe` with the SSL option to connect to the instance across the network through the firewall, it states that the connection has been refused. What port must you open on the firewall to allow you to connect to the AD LDS instance over SSL? Select the best answer.
- A. You need to open port 443 on the firewall to make this SSL connection.
  - B. You need to open port 53 on the firewall to make this SSL connection.
  - C. You need to open port 520 on the firewall to make this SSL connection.
  - D. You need to open port 636 on the firewall to make this SSL connection.

6. You are the network administrator for a small university in Kansas. You are responsible for the entire network, which consists of one Windows Server 2008 Active Directory domain. You have decided to make the university's web site internal and host it on your own servers. You want to use THREE servers to all host the same site; running Network Load Balancing (NLB) to route visitors to the first available server, in case the other servers are down or are too busy to serve up the site. All THREE servers have their own public static IP address, but you want visitors to connect to one IP address that will route to the first available server. When using NLB, what is the IP address called that routes traffic to the first available server? Select the best answer.
- A. That address is called a clustered IP address.
  - B. That address is called a bridgehead IP.
  - C. That address is called a PTR IP address, since it can point to any number of physical addresses.
  - D. That address is called a median address.
7. You are the systems administrator for your company. The network you administer is comprised of one 2008 Active Directory domain. You have one server still running Windows Server 2003 that was hosting the Rights Management Service (RMS) for the domain. You also have been using MSDE to host the RMS database. You upgraded the server to 2008, and now you need to upgrade the RMS cluster to Active Directory Rights Management Services (AD RMS). You log onto the server as an Enterprise Admin and start the upgrade to AD RMS. You receive multiple errors and the installation stops. What do you need to do to finish this upgrade to AD RMS? Select the best answer.
- A. You need to log on as a Schema Admin.
  - B. You need to install the newest version of MSDE before you can upgrade the RMS cluster.
  - C. You need to install AD RMS on another server and seize the role from the original RMS server.
  - D. You need to upgrade the MSDE database to a SQL server database before making the upgrade to AD RMS.
8. The company where you work is in the process of establishing a partnership relationship with another business. Windows Server 2008 Active Directory Federation Services servers have been installed and configured. You must configure the certificates for the federation servers. Which of the following steps are the correct sequence to complete this task? Select the best answer.
- A. 1. Create a server authentication certificate for the web server.  
2. Export the token-signing certificate from the account server to a file.  
3. Export the Server Certificate from the resource server to a file.  
4. Import the ADFS resource server authentication certificate to the web server.
  - B. 1. Create a server authentication certificate for the web server.  
2. Export the Server Certificate from the resource server to a file.  
3. Export the token-signing certificate from the account server to a file.  
4. Import the ADFS resource server authentication certificate to the web server.
  - C. 1. Create a server authentication certificate for the web server.  
2. Configure the trust policy.  
3. Add an Active Directory Account Store.  
4. Download certificates to the web server.
  - D. 1. Right-click Trust Policy in the ADFS dialog box.  
2. Select Properties.  
3. On the General tab type the path for the server in the Federation Service URI field.  
4. Verify that the correct URL appears in the Federation Service endpoint URL field.  
5. Enter the name of the trust on the Display Name tab.

9. You have been given the task of installing Windows Server 2008 Active Directory Federation Services at several remote offices for your company. All of the remote offices have the following server hardware on site -One Windows 2000 Server with a 133 MHz processor, 256 MB RAM, and 50 MB of free disk space -One Windows Server 2003 with a 133 MHz processor, 128 MB RAM, and 50 MB of free disk space -One Windows Server 2008 with a 1 GHz processor, 512 MB RAM, and 20 GB of free disk space Which of the following server configurations do NOT support ADFS? Choose all that apply.
- A. Install ADFS on the existing Windows Server 2008 system.
  - B. Install ADFS on the existing Windows Server 2003 system.
  - C. Add an additional 128 MB RAM to the existing Windows Server 2003 system and install ADFS.
  - D. Install ADFS on the existing Windows 2000 Server system.
10. Jenny is the senior network administrator for a small law firm in West Virginia. Every server in the firm's network is using Windows Server 2008 Enterprise. One of the developers in the IT staff has created a web application that allows associates to log in and check their open cases. These people are given an Active Directory account on the firm's network to authenticate them when they login. Jenny's firm has an agreement with another local law firm allowing them to use various office resources at Jenny's firm. The other firm's senior partner would like his associates to be able to log into the web application as well, to check case loads. Jenny definitely does NOT want the associates from the other firm to have Active Directory accounts in her network, so she sets up Active Directory Federated Services to allow the Active Directory accounts from the other firm to have access to the web application. After the initial setup, they find that the server running the Federated Services is being taxed too heavily, so Jenny decides to install TWO more servers with Federated Services. Jenny does NOT want to publish three URL's that would have access to the web application; she wants one address that associates can navigate to that would choose one server running Federated Services that is currently available. How would Jenny accomplish their task of using one name to gain access to any one of the three servers running Federated Services? Select the best answer.
- A. Jenny should install Active Directory Lightweight Directory Services on a server at the perimeter of her network. This would allow the associates to have an account on that server and use single-sign-on to access their information.
  - B. To enable one URL to point to any of the three servers, Jenny should edit the default.htm file on the first web server that was installed. Jenny needs to add the IPs of all three web servers to this file.
  - C. Jenny should use Microsoft Network Load Balancing to allow one address to point to any of the three web servers that is available. Network Load Balancing allows a clustered IP to point to a list of web servers' IPs.
  - D. Jenny should enable static cookies to all three web servers that would help redirect browsers to the appropriate web server.

## Chapter 2

1. Your organization consists of a single Active Directory forest in which servers run either Windows Server 2003 or Windows Server 2008 and all client computers run Windows Vista. Your network consists of two subnets and you plan to deploy a Windows Server 2008 DHCP server on each subnet. You need to ensure that neither server distributes a different IP address to the DHCP-enabled workgroup printers in the enterprise. What action should you perform?
  - A. Create a domain DFS in the forest.
  - B. Create an exclusion for the workgroup printers on both DHCP servers.
  - C. Create a reservation for the workgroup printers on one DHCP server.
  - D. Create a reservation for the workgroup printers on both DHCP servers.
  
2. Your network consists of a single Active Directory domain in which all servers run Windows Server 2008. You are deploying four additional file servers, all of which are configured with static IPv4 addresses. You need to ensure that the IP addresses that are statically assigned to the servers are NOT distributed to other hosts in the domain. What action should you perform?
  - A. Create a new exclusion range in DHCP.
  - B. Create reservations for the new servers in DHCP.
  - C. Configure the appropriate server option in DHCP.
  - D. Configure the appropriate scope option in DHCP.
  
3. Your organization consists of a multi-domain Active Directory forest in which all servers run Windows Server 2008 and all client computers run Windows Vista. Hosts in all domains are configured to use both IPv4 and IPv6. You need to ensure that hosts in different domains in the forest can communicate through networks that are separated by NAT firewalls. Your solution must involve the least amount of administrative effort. What action should you perform?
  - A. Enable the Peer Name Resolution Protocol (PNRP) on all organizational firewalls.
  - B. Enable Teredo on all organizational firewalls.
  - C. Create static NAT translation entries on all organizational firewalls.
  - D. Create at least one IPv6 scope on all DHCP servers.
  
4. Your organization consists of a single Active Directory domain in which all servers run either Windows Server 2003 or Windows Server 2008 and client computers run either Windows 2000 Professional or Windows XP SP2. You are planning to migrate the network's IP addressing infrastructure to IPv6. What actions should you perform? (Select TWO choices. Each correct answer represents a part of a single solution.)
  - A. Ensure that all DHCP servers are multihomed.
  - B. Ensure that all DHCP servers run Windows Server 2008.
  - C. Upgrade the Windows 2000 Professional computers to Windows XP SP2.
  - D. Upgrade the Windows Server 2003 computers to Windows Server 2008.

## Chapter 3

1. Your organization consists of a single Active Directory domain named Birdco.com. All servers in the domain run Windows Server 2008. You need to configure a Server Core member server named CORE01 to subscribe to hardware events that are generated by SRV01 and SRV02. These TWO member servers run a full installation of Windows Server 2008. You have created a subscription configuration file named subscrip.xml. What action should you perform next?
  - A. Create the hardware event subscription by using Event Viewer on CORE01.
  - B. Create that hardware event subscription by running the command `Wecutil cs subscrip.xml`.
  - C. Create a hardware event subscription by running a PowerShell cmdlet, specifying the subscrip.xml configuration file as an input parameter.
  - D. Create a hardware event subscription by running Netsh, specifying the subscrip.xml configuration file as an input file.
  
2. Your organization consists of a single Active Directory domain named Birdco.com in which all servers run Windows Server 2008. THREE of these servers, WSUS01, WSUS02, and WSUS03, are configured with Windows Server Update Services (WSUS). You need to configure WSUS such that all computer groups and approvals are configured at WSUS01 and updates are copied to WSUS02 and WSUS03. What action should you perform?
  - A. Configure WSUS02 and WSUS03 as upstream servers of WSUS01.
  - B. Configure WSUS02 and WSUS03 as downstream servers of WSUS01.
  - C. Configure WSUS01 as a disconnected server.
  - D. Configure WSUS02 and WSUS03 as replicas of WSUS01.
  
3. Your network consists of a single Active Directory domain in which all servers run Windows Server 2008 and all client workstations run Windows Vista. You manage the network from an administrative workstation named THOTH. You want to configure THOTH to receive Windows event log data from a domain controller named SERVER01. What actions should you perform? (Select TWO answers. Each correct answer represents a part of a single solution).
  - A. Run the `winrm quickconfig` command on THOTH.
  - B. Run the `winrm quickconfig` command on SERVER01.
  - C. Run the `wecutil` command on THOTH.
  - D. Run the `wecutil` command on SERVER01.

## Chapter 4

1. You are configuring WDS for image deployment. As part of this process, you must select a volume for image storage. You have four choices: C: - NTFS - 4 GB free - operating system volume D: - FAT32 - 12 GB free - data volume E: - NTFS - 100 GB free - data volume F: - FAT32 - 16 GB free - data volume You may select any of the volumes, but you want the best performance possible. Which volume will you choose? Select the best answer.
  - A. C:
  - B. D:
  - C. E:
  - D. F:
2. You work as an administrator in an environment with very high security requirements. The organizational policy dictates that operating systems and applications can only be deployed to pre-staged machines. You are configuring WDS and have to choose the PXE Server Initial Settings, which define the answer policy for the WDS server. Which answer policy will you choose in order to comply with the organizational policy and allow for automatic deployment of operating systems to pre-staged computers? Select the best answer.
  - A. Do not respond to any client computer.
  - B. Respond only to known client computers.
  - C. Respond only to pre-staged computers.
  - D. Respond to all (known and unknown) client computers.

## Chapter 5

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 Remote Desktop Web Connection
  - B. TS RemoteApp
  - C. Remote Desktop
  - D. Remote Registry
2. 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



3. You want to implement load balancing and support session reconnection even if the user connects from a different client than the client used to originally establish the session. You plan to implement Session Broker. What editions of Windows Server 2008 support the TS Session Broker? Choose all that apply.
- A. Windows Server 2008 Web Edition
  - B. Windows Server 2008 Standard Edition
  - C. Windows Server 2008 Enterprise Edition
  - D. Windows Server 2008 Datacenter Edition

## Chapter 6

1. You have been asked to create a batch file that will be scheduled in order to perform backups for the company's website. The website is hosted on an IIS 7 server running Windows 2008 Server as the operating system. You have written the needed batch file commands to backup the website data. Now, you need to ensure that the IIS 7 configuration information is backed up into a text file. Which command will you use for this? Select the best answer.
- A. AppCmd
  - B. Backup
  - C. IISBack
  - D. NetBack
2. You are implementing a web application using IIS 7. Configuration files apply in a specific hierarchy and the lower-level configuration files may override the upper-level files. Which of the following represents the appropriate hierarchy of configuration files listed from upper-level to lower-level? Select the best answer.
- A. ApplicationHost.config, Web.config (site), Web.config (application).
  - B. Web.config (site), ApplicationHost.config, Web.config (application).
  - C. Web.config (application), ApplicationHost.config, Web.config (site).
  - D. Web.config (site), Web.config (application), ApplicationHost.config.
3. You have an older web application that makes called to the IIS 6.0 and earlier metabase. What is the name of the layer that interprets older metabase calls so that they can be mapped to the new ApplicationHost.config files? Select the best answer.
- A. Admin Base Object Mapper
  - B. Active Data Object Mapper
  - C. INI Compatibility Layer
  - D. Registry Mapper

# Answers & Explanations

## Chapter 1

### 1. Answers: A

**Explanation A.** Correct. The forest functional level must be Windows Server 2003, so that linked-value replication is available. This provides a higher level of replication consistency.

Explanation B. Incorrect. You must be logged on as an Enterprise Admin to run `adprep /rodcrep`.

Explanation C. Incorrect. This command can be run on any computer in a domain that has a connection to the domain controller with the infrastructure master operations role.

Explanation D. Incorrect. This option is not necessary to enable the `adprep /rodcrep` command to function properly.

### 2. Answers: D

Explanation A. Incorrect. While this would provide single-sign-on access for the students, it would not allow one URL to point to any of the three servers running Federated Services.

Explanation B. Incorrect. Adding the IPs of the servers to this file would not do anything.

Explanation C. Incorrect. Static cookies would not enable one URL to point to any one of the three servers that is available.

**Explanation D.** Correct. Network Load Balancing would allow one host name to be redirected to the first available web server hosting the web application.

### 3. Answers: B

Explanation A. Incorrect. Windows Server 2003 is supported. Configuring Additional Active Directory Server Roles 28.

**Explanation B.** Correct. This setting must be changed so that the guest operating systems can boot properly.

Explanation C. Incorrect. This feature must be enabled in the BIOS for the hypervisor to boot.

Explanation D. Incorrect. The NIC has nothing to do with the guest operating system booting properly.

#### 4. Answers: A

**Explanation A.** Correct. Network Access Protection (NAP) is new in Windows Vista and Windows Server 2008 and allows for the creation of security policies and standards that computers must comply with to gain access to a network.

Explanation B. Incorrect. While WSUS helps computers stay up-to-date with Microsoft patches, it does not ensure that they are compliant with security policies before logging onto a network.

Explanation C. Incorrect. IPSec is used to create secure tunnels between devices, not to ensure whether devices are secure enough to allow onto a network.

Explanation D. Incorrect. While using certificates to verify user or computer accounts is a good security policy, it would not check for current patches or virus updates.

#### 5. Answers: D

Explanation A. Incorrect. Port 443 is only used in SSL when connecting over HTTPS, not LDAP.

Explanation B. Incorrect. Port 53 is used for DNS traffic, not secure LDAP.

Explanation C. Incorrect. Port 520 is used for RIP.

**Explanation D.** Correct. This is the port used by secure LDAP.

#### 6. Answers: A

**Explanation A.** Correct. A clustered IP address is configured on each server in a cluster so visitors can navigate to one IP address.

Explanation B. Incorrect. This is a clustered IP address.

Explanation C. Incorrect. A PTR record is used in DNS for pointing an IP address to a host name.

Explanation D. Incorrect. There is no such thing as a median IP address.

#### 7. Answers: D

Explanation A. Incorrect. Enterprise Admins have sufficient permission.

Explanation B. Incorrect. When upgrading to AD RMS, MSDE must be upgraded to SQL server.

Explanation C. Incorrect. AD RMS is not a forest- or domain-level master role and cannot be seized.

**Explanation D.** Correct. This upgrade must be made before upgrading the RMS cluster to AD RMS.

## 8. Answers: A

**Explanation A.** Correct. This is the correct sequence of steps to complete this task.

Explanation B. Incorrect. This is not the correct sequenced of steps in order to complete this task. You must export the token-signing certificate from the account server before you export the Server Certificate.

Explanation C. Incorrect. This is not the correct sequenced of steps in order to complete this task. Most of these steps would need to be completed when you are configuring the Resource Federation server.

Explanation D. Incorrect. These are the steps you would follow in order to create a Configuring Additional Active Directory Server Roles 30 trust on an ADFS server.

## 9. Answers: B, D

Explanation A. Incorrect. The configuration of the server running Windows Server 2008 more than meets the minimum requirements for installing ADFS.

**Explanation B.** Correct. The server running Windows Server 2003 does not have the minimum requirement of RAM to support ADFS. You must have a minimum of 256 MB RAM in order to install ADFS.

Explanation C. Incorrect. By adding RAM to the existing Windows Server 2003 system you would be able to install ADFS.

**Explanation D.** Correct. ADFS can only run on Windows Server 2003 R2 Enterprise Edition, Windows Server 2003 R2 Datacenter Edition, Windows Server 2008 Enterprise, or Windows Server 2008 Datacenter. It can not run on earlier operating systems.

## 10. Answers: C

Explanation A. Incorrect. While this would provide single-sign-on access for the associates, it would not allow one URL to point to any of the three servers running Federated Services.

Explanation B. Incorrect. Adding the IPs of the servers to this file would not do anything.

**Explanation C.** Correct. Network Load Balancing would allow one host name to be redirected to the first available web server hosting the web application.

Explanation D. Incorrect. Static cookies would not enable one URL to point to any one of the three servers that is available.

## Chapter 2

### 1. Answers: D

Explanation A. Incorrect. Here, we are concerned with IP address configuration (DHCP), not making file-system resources available in a redundant way (Distributed File System or DFS).

Explanation B. Incorrect. An exclusion removes one or more IP addresses from a DHCP scope. The scenario in this case states explicitly that the workgroup printers are DHCP clients.

Explanation C. Incorrect. If we perform this action, there exists the possibility that the workgroup printers, which are configured as DHCP clients, may pick up a different IP address from the other DHCP server.

**Explanation D.** Correct. When you have multiple DHCP servers in an enterprise, you need to be careful to plan and create scopes, keeping in mind that the servers never synchronize their scope data. The configurations must be manually duplicated on all servers.

### 2. Answers: A

**Explanation A.** Correct. An exclusion range removes one or more IP addresses from a DHCP scope, ensuring that DHCP will never offer those addresses to DHCP clients.

Explanation B. Incorrect. Because the scenario states that the new servers are configured with static IP addresses, client reservations will not work in this situation.

Explanation C. Incorrect. There exists no scope or server option that would prevent duplicate addresses from being delivered. We need to use either exclusions or client reservations.

Explanation D. Incorrect. Scope and/or server options will not help us solve the problem that is outlined in this scenario.

### 3. Answers: B

Explanation A. Incorrect. PNRP is an IPv6-based discover technology that underpins Microsoft applications such as Meeting Space. However, without Teredo enabled on all firewalls, the firewalls will not let IPv6 packets traverse NAT.

**Explanation B.** Correct. Teredo technology allows IPv6 packets to traverse IPv4 Network Address Translation (NAT) firewalls. The Teredo client is enabled by default in Windows Server 2008 and Windows Vista.

Explanation C. Incorrect. Although this would solve the problem, it is almost mind-numbingly complex compared to enabling Teredo on all firewalls.

Explanation D. Incorrect. This answer choice represents a classic “red herring.” That is, we don’t need to worry about IP addressing. There is nothing in the scenario that would lead us to believe there is a problem with addressing.

#### 4. Answers: B, C

Explanation A. Incorrect. There is no requirement for this in order for a Windows Server 2008 DHCP server to support a dual IPv4/IPv6 infrastructure.

**Explanation B.** Correct. Although Windows Server 2003 R2 can use IPv6 as a client, only Windows Server 2008 DHCP includes support for IPv6 scopes.

**Explanation C.** Correct. IPv6 is not available in Windows 2000 or Windows 9x.

Explanation D. Incorrect. Windows Server 2003 includes native support for IPv6.

### Chapter 3

#### 1. Answers: B

Explanation A. Incorrect. Remember that CORE01 is a Server Core installation of Windows Server 2008. Therefore, we must use the Wecutil command-line utility to manage the Event Collector service.

**Explanation B.** Correct. We can use the Wecutil cs command to define an event subscription by supplying a previously created hardware event collector subscription file in Extensible Markup Language (XML) format.

Explanation C. Incorrect. Server Core installations of Windows Server 2008 do not support PowerShell.

Explanation D. Incorrect. The Network Shell utility is used to manage network settings only.

#### 2. Answers: B

Explanation A. Incorrect. We want just the opposite; that is to say, WSUS01 configured as the upstream server, and WSUS02 and WSUS03 configured as downstream servers.

**Explanation B.** Correct. The upstream WSUS server downloads updates from Microsoft.com and stores global configuration data. Only the updates and metadata are downloaded from the upstream WSUS server to the downstream WSUS servers.

Explanation C. Incorrect. You can manually export updates and metadata from one WSUS server and apply them manually to another WSUS server that is disconnected from the network. This is not what we want to do in this scenario.

Explanation D. Incorrect. In a replica scenario, computer groups and other data that we want to keep centralized is replicated to the other WSUS servers in the topology. In this case, we want only updates to be spread across all servers, not global configuration data.

### 3. Answers: B, C

Explanation A. Incorrect. This command enables the Windows Remote Management service which needs to be running in order for a host to forward its event log data. However, we need to run this command on SERVER01, not THOTH.

**Explanation B.** Correct. We could use either Group Policy or the winrm command to enable the Windows Remote Management service on the target computer(s).

**Explanation C.** Correct. The Wecutil command is a command-line utility that can be used to create and manage event subscriptions. Alternatively, we could use Event Viewer to create the subscription.

Explanation D. Incorrect. Because our Windows Vista-based administrative workstation is running the Event Collector service, we need to create the subscriptions on this computer, not the server that will be forwarding its events.

## Chapter 4

### 1. Answers: C

Explanation A. Incorrect. Using the operating system volume is not recommended for performance reasons. Additionally, 4 GB is not likely to be sufficient storage space.

Explanation B. Incorrect. You must use an NTFS volume for image storage.

**Explanation C.** Correct. This is an NTFS volume, which is required, and it has sufficient free space.

Explanation D. Incorrect. You must use an NTFS volume for image storage.

### 2. Answers: B

Explanation A. Incorrect. This option would not allow for the automatic deployment of operating systems to any clients. This state is similar to parking the server for future use.

**Explanation B.** Correct. This option will only allow computers that are pre-staged in Active Directory to receive automated operating system installations. A pre-staged computer is a computer that has been created in the AD database by an administrator.

Explanation C. Incorrect. There is no such option in the PXE Server Initial Settings dialog. The "Respond only to known client computers" is the appropriate choice.

Explanation D. Incorrect. While this will allow for the automated installation of operating systems, it will not prevent installation on computers that are not pre-staged.

## Chapter 5

### 1. Answers: A

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

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. 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.

### 3. Answers: B, C, D

Explanation A. Incorrect. This edition does not support Session Broker or Terminal Services.

**Explanation B.** Correct. Windows Server 2008 Standard, Enterprise and Datacenter Configuring Terminal Services 37 editions all support Session Broker. In Windows Server 2003, only the Enterprise and Datacenter editions supported the Session Directory, which was similar to Session Broker.

**Explanation C.** Correct. Windows Server 2008 Standard, Enterprise and Datacenter editions all support Session Broker. In Windows Server 2003, only the Enterprise and Datacenter editions supported the Session Directory, which was similar to Session Broker.

**Explanation D.** Correct. Windows Server 2008 Standard, Enterprise and Datacenter editions all support Session Broker. In Windows Server 2003, only the Enterprise and Datacenter editions supported the Session Directory, which was similar to Session Broker.

## Chapter 6

### 1. Answers: A

**Explanation A.** Correct. Using a command such as AppCmd add backup "IISConfig" will backup the IIS configuration data to a file named IISConfig. Note that the command is AppCmd add backup "BackupName".

Explanation B. Incorrect. The Backup command provides no unique features for backup up IIS configuration data.

Explanation C. Incorrect. No such command exists.

Explanation D. Incorrect. No such command exists.



## 2. Answers: A

**Explanation A.** Correct. The host is first and these settings are global, but they may be overridden by the lower levels. Next is the Web.config for the site and finally the Web.config for the application.

Explanation B. Incorrect. The proper sequence is ApplicationHost.config, Web.config (site), Web.config (application).

Explanation C. Incorrect. The proper sequence is ApplicationHost.config, Web.config (site), Web.config (application).

Explanation D. Incorrect. The proper sequence is ApplicationHost.config, Web.config (site), Web.config (application).

## 3. Answers: A

**Explanation A.** Correct. The ADO Mapper allows for metabase calls to be redirected to the appropriate section of the ApplicationHost.config file.

Explanation B. Incorrect. While ADO is a real concept, there is no such feature as the Configuring a Web Services Infrastructure 39 ADO Mapper.

Explanation C. Incorrect. IIS 6 and earlier did not use INI files for the metabase.

Explanation D. Incorrect. IIS 6 and earlier did not use the registry for metabase information.