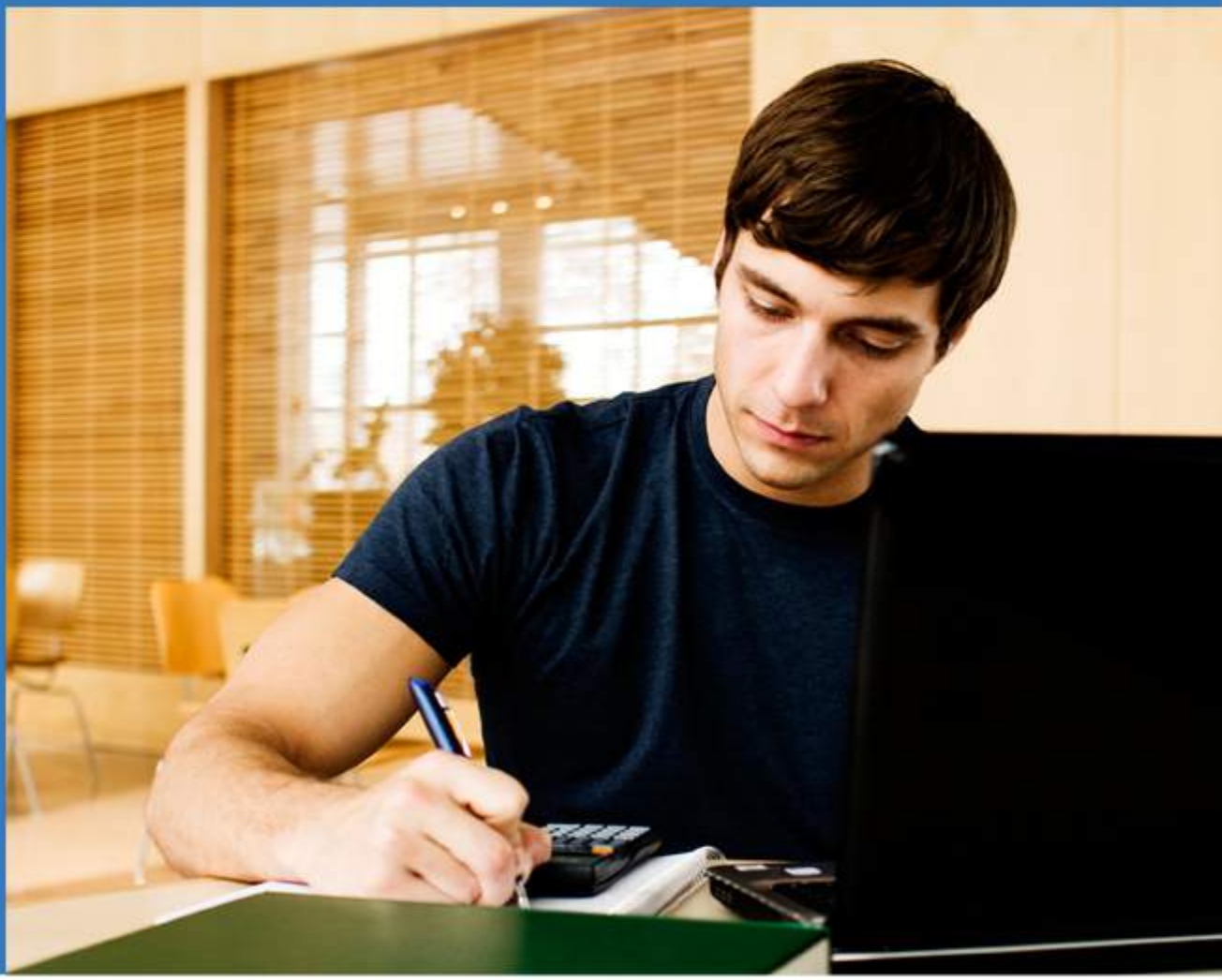
Study Guide

Microsoft Windows Server 2008 Functionality Changes

Powered by Microsoft|TechNet



ExamForce

Table of Contents

Chapter 1 – What's New in Active Directory Certificate Services

Chapter 1

What are the major changes?

Active Directory® Certificate Services (AD CS) in Windows Server® 2008 R2 introduces features and services that allow more flexible public key infrastructure (PKI) deployments, reduce administration costs, and provide better support for Network Access Protection (NAP) deployments.

The AD CS features and services in the following table are new in Windows Server 2008 R2.

Feature	Benefit
Certificate Enrollment Web Service and Certificate Enrollment Policy Web Service	Enables certificate enrollment over HTTP.
Support for certificate enrollment across forests	Enables certification authority (CA) consolidation in multiple-forest deployments.
Improved support for high-volume CAs	Reduced CA database sizes for some NAP deployments and other high-volume CAs.

Certificate Enrollment Web Service and Certificate Enrollment Policy Web Service

The certificate enrollment Web services are new AD CS role services that enable policy-based certificate enrollment over HTTP by using existing methods such as autoenrollment. The Web services act as a proxy between a client computer and a CA, which makes direct communication between the client computer and CA unnecessary, and allows certificate enrollment over the Internet and across forests.

Who will be interested in this feature?
Organizations with new and existing PKIs can benefit from the expanded accessibility of certificate enrollment provided by the certificate enrollment Web services in these deployment scenarios:

- In multiple-forest deployments, client computers can enroll for certificates from CAs in a different forest.
- In extranet deployments, mobile workers and business partners can enroll over the Internet.

Are there any special considerations?
The Certificate Enrollment Web Service submits requests on behalf of client computers and must be trusted for delegation. Extranet deployments of this Web service increase the threat of network attack, and some organizations might choose not to trust the service for delegation. In these cases, the Certificate Enrollment Web Service and issuing CA can be configured to accept only renewal requests signed with existing certificates, which does not require delegation.

The certificate enrollment Web services also have the following requirements:

- Active Directory forest with Windows Server 2008 R2 schema.
- Enterprise CA running Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003.
- Certificate enrollment across forests requires an enterprise CA running the Enterprise or Datacenter edition of Windows Server.
- Client computers running Windows® 7.

Which editions include this feature?
The certificate enrollment Web services are available in all editions of Windows Server 2008 R2.

Support for certificate enrollment across forests

Before the introduction of enrollment across forests, CAs could issue certificates only to members of the same forest, and each forest had its own PKI. With added support for LDAP referrals, Windows Server 2008 R2 CAs can issue certificates across forests that have two-way trust relationships.

Who will be interested in this feature?
Organizations with multiple Active Directory forests and per-forest PKI deployments can benefit from CA consolidation by enabling certificate enrollment across forests.

Are there any special considerations?

- Active Directory forests require Windows Server 2003 forest functional level and two-way transitive trust.
- Client computers running Windows XP, Windows Server 2003, and Windows Vista® do not require updates to support certificate enrollment across forests.

Which editions include this feature?
This feature is available on enterprise CAs running Windows Server 2008 R2 Enterprise or Windows Server 2008 R2 Datacenter.

Improved support for high-volume CAs

Who will be interested in this feature?
Organizations that have deployed NAP with IPsec enforcement or other high-volume CAs can choose to bypass certain CA database operations to reduce CA database size.

NAP health certificates typically expire within hours after being issued, and the CA might issue multiple certificates per computer each day. By default, a record of each request and issued certificate is stored in the CA database. A high volume of requests increases the CA database growth rate and administration cost.

Are there any special considerations?
Because issued certificates are not stored in the CA database, certificate revocation is not possible. However, maintenance of a certificate revocation list for a high volume of short-lived certificates is often not practical or beneficial. As a result, some organizations might choose to use this feature and accept the limitations on revocation.

Chapter 2 – What's New in Active Directory Domain Services

What are the major changes?

Active Directory® Domain Services (AD DS) in the Windows Server® 2008 R2 operating system includes many new features that help improve Active Directory manageability, supportability, and performance.

The following changes are available in Windows Server 2008 R2:

- Active Directory Recycle Bin

  Information technology (IT) professionals can use Active Directory Recycle Bin to undo an accidental deletion of an Active Directory object. Accidental object deletion causes business downtime. Deleted users cannot log on or access corporate resources. This is the number one cause of Active Directory recovery scenarios. Active Directory Recycle Bin works for both AD DS and Active Directory Lightweight Directory Services (AD LDS) objects. This feature is enabled in AD DS at the Windows Server 2008 R2 forest functional level. For AD LDS, all replicas must be running in a new "application mode." For more information, see What's New in AD DS: Active Directory Recycle Bin.

- Active Directory module for Windows PowerShell and Windows PowerShell™ cmdlets

  The Active Directory module for Windows PowerShell provides command-line scripting for administrative, configuration, and diagnostic tasks, with a consistent vocabulary and syntax. It provides predictable discovery and flexible output formatting. You can easily pipe cmdlets to build complex operations. The Active Directory module enables end-to-end manageability with Exchange Server, Group Policy, and other services. For more information, see What's New in AD DS: Active Directory Module for Windows PowerShell.

- Active Directory Administrative Center

  The Active Directory Administrative Center has a task-oriented administration model, with support for larger datasets. The Active Directory Administrative Center can help increase the productivity of IT professionals by providing a scalable, task-oriented user experience for managing AD DS. In the past, the lack of a task-oriented user interface (UI) could make certain activities, such as resetting user passwords, more difficult than they had to be. The Active Directory Administrative Center enumerates and organizes the activities that you perform when you manage a system. These activities may be maintenance tasks, such as backup; event-driven tasks, such as adding a user; or diagnostic tasks that you perform to correct system failures. For more information, see What's New in AD DS: Active Directory Administrative Center.

- Active Directory Best Practices Analyzer

  The Active Directory Best Practices Analyzer (BPA) identifies deviations from best practices to help IT professionals better manage their Active Directory deployments. BPA uses Windows PowerShell cmdlets to gather run-time data. It analyzes Active Directory settings that can cause unexpected behavior. It then makes Active Directory configuration recommendations in the context of your deployment. The Active Directory BPA is available in Server Manager. For more information, see What's New in AD DS: Active Directory Best Practices Analyzer.

- Active Directory Web Services

  Active Directory Web Services (ADWS) provides a Web service interface to Active Directory domains and AD LDS instances, including snapshots, that are running on the same Windows Server 2008 R2 server as ADWS. For more information, see What's New in AD DS: Active Directory Web Services.

- Authentication mechanism assurance

  Authentication mechanism assurance makes it possible for applications to control resource access based on authentication strength and method. Administrators can map various properties, including authentication type and authentication strength, to an identity. Based on information that is obtained during authentication, these identities are added to Kerberos tickets for use by applications. This feature is enabled at the Windows Server 2008 R2domain functional level. For more information, see What's New in AD DS: Authentication Mechanism Assurance.

- Offline domain join

  Offline domain join makes provisioning of computers easier in a datacenter. It provides the ability to preprovision computer accounts in the domain to prepare operating system images for mass deployment. Computers are joined to the domain when they first start. This reduces the steps and time necessary to deploy computers in a datacenter. For more information, see What's New in AD DS: Offline Domain Join.

- Managed Service Accounts

  Managed Service Accounts provide simple management of service accounts. At the Windows Server 2008 R2 domain functional level, this feature provides better management of service principal names (SPNs). Managed Service Accounts help lower total cost of ownership (TCO) by reducing service outages (for manual password resets and related issues). You can run one Managed Service Account for each service that is running on a server, without any human intervention for password management.

- Active Directory Management Pack

  The Active Directory Management Pack enables proactive monitoring of availability and performance of AD DS. It discovers and detects computer and software states, and it is aligned with the health state definitions. The Active Directory Management Pack works with Windows Server 2008 and Windows Server 2008 R2 and Microsoft® Systems Center Operations Manager 2007.

What's New in AD DS: Active Directory Recycle Bin

What are the major changes?

Accidental deletion of Active Directory objects is a common occurrence for users of Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS).

In Windows Server 2008 Active Directory domains, you could recover accidentally deleted objects from backups of AD DS that were taken by Windows Server Backup. You could use the **ntdsutil** authoritative restore command to mark objects as authoritative to ensure that the restored data was replicated throughout the domain. The drawback to the authoritative restore solution was that it had to be performed in Directory Services Restore Mode (DSRM). During DSRM, the domain controller being restored had to remain offline. Therefore, it was not able to service client requests.

Also, in Windows Server 2003 Active Directory and Windows Server 2008 AD DS, you could recover deleted Active Directory objects through tombstone reanimation. In Windows Server 2003 and Windows Server 2008, a deleted Active Directory object was not physically removed from the database immediately. Instead, the object's distinguished name (also known as DN) was mangled, most of the object's non-link-valued attributes were cleared, all of the object's link-valued attributes were physically removed, and the object was moved to a special container in the object's naming context (also known as NC) named Deleted Objects. The object, now called a tombstone, became invisible to normal directory operations. Tombstones could be reanimated anytime within the tombstone lifetime period and become live Active Directory objects again. The default tombstone lifetime was 180 days in Windows Server 2003 and Windows Server 2008. You could use tombstone reanimation to recover deleted objects without taking your domain controller or your AD LDS instance offline. However, reanimated objects' link-valued attributes (for example, group memberships of user accounts) that were physically removed and non-link-valued attributes that were cleared were not recovered. Therefore, administrators could not rely on tombstone reanimation as the ultimate solution to accidental deletion of objects.

Active Directory Recycle Bin in Windows Server 2008 R2 builds on the existing tombstone reanimation infrastructure and enhances your ability to preserve and recover accidentally deleted Active Directory objects

Windows Server 2008 R2 Active Directory Recycle Bin helps minimize directory service downtime by enhancing your ability to preserve and restore accidentally deleted Active Directory objects without restoring Active Directory data from backups, restarting AD DS, or rebooting domain controllers.

What does Active Directory Recycle Bin do?

When you enable Active Directory Recycle Bin, all link-valued and non-link-valued attributes of the deleted Active Directory objects are preserved and the objects are restored in their entirety to the same consistent logical state that they were in immediately before deletion. For example, restored user accounts automatically regain all group memberships and corresponding access rights that they had immediately before deletion, within and across domains. Active Directory Recycle Bin works for both AD DS and AD LDS environments.

What's New in AD DS: Active Directory Module for Windows PowerShell

What are the major changes?

The Active Directory module for Windows PowerShell provides command-line scripting for administrative, configuration, and diagnostic tasks, with a consistent vocabulary and syntax. The Active Directory module enables end-to-end manageability with Exchange Server, Group Policy, and other services.

What does the Active Directory module do?

Windows PowerShell™ is a command-line shell and scripting language that can help information technology (IT) professionals control system administration more easily and achieve greater productivity.

The Active Directory module in Windows Server 2008 R2 is a Windows PowerShell module (named Active Directory) that consolidates a group of cmdlets. You can use these cmdlets to manage your Active Directory domains, Active Directory Lightweight Directory Services (AD LDS) configuration sets, and Active Directory Database Mounting Tool instances in a single, self-contained package.

In Windows Server 2000, Windows Server 2003, and Windows Server 2008, administrators used a variety of command-line tools and Microsoft Management Console (MMC) snap-ins to connect to their Active Directory domains and AD LDS configuration sets to monitor and manage them. The Active Directory module in Windows Server 2008 R2 now provides a centralized experience for administering your directory service.

What's New in AD DS: Active Directory Administrative Center

What are the major changes?

In the Windows Server 2003 and Windows Server 2008 operating systems, administrators could manage and publish information in their Active Directory environments by using the Active Directory Users and Computers Microsoft Management Console (MMC) snap-in. In Windows Server 2008 R2, in addition to the Active Directory Users and Computers snap-in, administrators can manage their directory service objects by using the new Active Directory Administrative Center.

Built on Windows PowerShell technology, Active Directory Administrative Center provides network administrators with an enhanced Active Directory data management experience and a rich graphical user interface (GUI). Administrators can use Active Directory Administrative Center to perform common Active Directory object management tasks through both data-driven navigation and task-oriented navigation.

You can use Active Directory Administrative Center to perform the following Active Directory administrative tasks:

- Create new user accounts or manage existing user accounts
- Create new groups or manage existing groups
- Create new computer accounts or manage existing computer accounts
- Create new organizational units (OUs) and containers or manage existing OUs
- Connect to one or several domains or domain controllers in the same Active Directory Administrative Center instance and view or manage the directory information for those domains or domain controllers
- Filter Active Directory data by using query-building search

In addition to using it for these tasks, you can use the enhanced Active Directory Administrative Center GUI to customize Active Directory Administrative Center to suite your particular requirements for directory service administration. This can help improve your productivity and efficiency as you perform common Active Directory object management tasks.

Are there any special considerations?

- Active Directory Administrative Center can be installed only on computers running the Windows Server 2008 R2 operating system. Active Directory Administrative Center cannot be installed on computers running Windows 2000, Windows Server 2003, or Windows Server 2008.
- Active Directory Administrative Center can be installed on the Windows 7 operating system as part of the Remote Server Administration Tools (RSAT).
- In this release of Windows Server 2008 R2, you cannot use Active Directory Administrative Center to manage Active Directory Lightweight Directory Services (AD LDS) instances and configuration sets.

What new functionality does Active Directory Administrative Center provide?

Active Directory Administrative Center includes the following new features:

- **Administrative Center Overview page**: This welcome page appears by default when you first open Active Directory Administrative Center. The Administrative Center Overview page consists of several tiles, each of which features an administrative task that you perform frequently, such as resetting a user password or searching through Active Directory data. You can customize the Administrative Center Overview page anytime by displaying or hiding various tiles.

- **Management of Active Directory objects across multiple domains**: When you open Active Directory Administrative Center on your Windows Server 2008 R2 server, the domain that you are currently logged on to on this Windows Server 2008 R2 server (the local domain) appears in the Active Directory Administrative Center navigation pane. Depending on the rights of your current set of logon credentials, you can view or manage the Active Directory objects in this local domain. You can also use the same instance of Active Directory Administrative Center and the same set of logon credentials to view or manage Active Directory objects from any other domain (that belongs or does not belong to the same forest as the local domain) as long as it has an established trust with the local domain (Both one-way trusts and two-way trusts are supported.)

- **Active Directory Administrative Center navigation pane**: You can browse through the Active Directory Administrative Center navigation pane by using the Tree view, which is similar to the Active Directory Users and Computers console tree, or by using the new list view:

    - In the list view, you can take advantage of the Column Explorer feature. Column Explorer simplifies your browsing through the various levels of your Active Directory hierarchy by displaying all the child containers of a parent container, for which you opened Column Explorer, in a single column.

    - In the list view, you can take advantage of the Most Recently Used (MRU) list. The MRU list automatically appears under a navigation node when you visit at least one container within this navigation node. The MRU list always contains the last three containers that you visited in a particular navigation node. Every time that you select a particular container, this container is added to the top of the MRU list and the last container in the MRU list is removed from it.

    - Whether you use the tree view or the list view, you can customize your Active Directory Administrative Center navigation pane anytime by adding various containers from the local domain or any foreign domain (that is, a domain other than the local domain that has an established trust with the local domain) to the navigation pane as separate nodes. Also, to further customize the navigation pane, you can rename or remove these manually added navigation pane nodes, create duplicates of these nodes, or move them up or down in the navigation pane.

    - In Active Directory Administrative Center, you can use different domain controllers to manage your Active Directory domains. You can change a domain controller connection for any node in the navigation pane. However, changing a domain controller connection for any particular node that represents a container within a certain domain also changes that connection for all other nodes in the navigation pane that represent containers that belong to that same domain.

- **Active Directory Administrative Center breadcrumb bar**: You can use the breadcrumb bar to navigate directly to the container that you want to view by specifying the distinguished name of the container in the breadcrumb bar.

- **Active Directory Administrative Center object property page**: The object property page consists of several property page sections and an inline preview feature. You can display, hide, or collapse any property page sections and the inline preview to customize your Active Directory Administrative Center object property page.

- **Active Directory Administrative Center query-building search**: Instead of spending hours browsing through levels of hierarchical data, you can quickly locate Active Directory objects by using query-building search in Active Directory Administrative Center. When the targeted Active Directory objects are returned as the results of a search query, you can perform the necessary administrative tasks. To use Active Directory Administrative Center query-building search, you can use the following methods:

    - You can use Active Directory Administrative Center Global Search to specify a scope for your search query. The default Global Search scope is set to the local domain. You can use Global Search to search through your Active Directory data by either building a query using keywords and various search criteria or by using the Lightweight Directory Access Protocol (LDAP) query mode.

    - If an OU contains a particularly large data set, you can narrow it down by building a query and searching through the Active Directory data of that specific OU. The scope of the search through the Active Directory data of a specific OU is always set to that particular OU, it and cannot be adjusted. This scope also does not include any OUs that are children of the selected parent OU.

    - When you use Global Search or when you search the data of a specific OU, you can save the queries that you build as separate views and use them again at a later time. Each view consists of your query criteria, as well as your customized sorting and column information.

What's New in AD DS: Active Directory Best Practices Analyzer

What are the major changes?

Best Practices Analyzer (BPA) is a server management tool that is available in Windows Server 2008 R2 for the following server roles:

- Active Directory Domain Services (AD DS)

- Active Directory Certificate Services (AD CS)

- DNS Server

- Terminal Services

AD DS BPA can help you implement best practices in the configuration of your Active Directory environment. AD DS BPA scans the AD DS server role as it is installed on your Windows Server 2008 R2 domain controllers, and it reports best practice violations. You can filter or exclude results from AD DS BPA reports that you do not need to see. You can also perform AD DS BPA tasks by using either the Server Manager graphical user interface (GUI) or cmdlets in the Windows PowerShell command-line interface

What new functionality does AD DS BPA provide?

Server Manager in Windows Server 2008 R2 includes a BPA engine that can run the AD DS BPA service. The AD DS BPA service consists of the following components:

- AD DS BPA Windows PowerShell script: The script collects AD DS configuration data and stores it in an XML document.
- XML schema: The schema defines the format, which follows the logical structure of the directory, of the XML document that the AD DS BPA Windows PowerShell script produces.
- AD DS BPA rules: The rules define the best-practice configuration for an AD DS environment.
- AD DS BPA guidance: This information can help administrators make adjustments to their AD DS environment to comply with the best practice configuration.

When you run the AD DS BPA scan on a domain controller, the BPA engine invokes the AD DS BPA Windows PowerShell script that collects configuration data from the AD DS environment that this domain controller belongs to.

The AD DS BPA Windows PowerShell script then saves the collected AD DS configuration data to an XML document. The BPA run-time engine validates this XML document against the XML schema.

Next, the BPA engine applies each rule in the AD DS BPA rules set to this XML document. If the configuration data in the XML document does not violate the best practice that is defined in a particular AD DS BPA rule, this rule appears as compliant in the Server Manager GUI.

If the BPA engine detects a best-practice violation in the XML document against a particular AD DS BPA rule, the corresponding noncompliant guidance for that rule appears in the Server Manager GUI. The noncompliant guidance for each AD DS BPA rule includes a description of the AD DS BPA violation (the problem), a description of the impact that this violation can have on the rest of your AD DS environment, and a recommendation regarding how to resolve the AD DS BPA violation.

How should I prepare to deploy AD DS BPA?

The AD DS BPA service is installed automatically when AD DS is installed on a computer that is running the Windows Server 2008 R2 and that computer becomes a domain controller. This includes both writable domain controllers and read-only domain controllers (RODCs). No other preparations are required.

What's New in AD DS: Active Directory Web Services

What does Active Directory Web Services do?

Active Directory Web Services (ADWS) in Windows Server 2008 R2 is a new Windows service that provides a Web service interface to Active Directory domains, Active Directory Lightweight Directory Services (AD LDS) instances, and Active Directory Database Mounting Tool instances that are running on the same Windows Server 2008 R2 server as ADWS. If the ADWS service on a Windows Server 2008 R2 server is stopped or disabled, client applications, such as the Active Directory module for Windows PowerShell or the Active Directory Administrative Center will not be able to access or manage any directory service instances that are running on this server.

ADWS is installed automatically when you add the AD DS or AD LDS server roles to your Windows Server 2008 R2 server. ADWS is configured to run if you make this Windows Server 2008 R2 server a domain controller by running Dcpromo.exe or if you create an AD LDS instance on this Windows Server 2008 R2 server.

What new functionality does ADWS provide?

In ADWS, there are a number of configuration parameters that determine how ADWS in Windows Server 2008 R2 handles the traffic that administrators generate. Administrators can manage AD DS domains, AD LDS instances, and Active Directory Database Mounting Tool instances by using applications such as the Active Directory module or Active Directory Administrative Center. These configuration parameters are stored in the Microsoft.ActiveDirectory.WebServices.exe.config file, under %WINDIR%\ADWS directory.

You can adjust these configuration parameters by editing the Microsoft.ActiveDirectory.WebServices.exe.config file to accommodate traffic that is directed at the ADWS service in their Active Directory environments. Any changes that you make to the ADWS configuration parameters on a given domain controller affect only the ADWS service that is running on this particular domain controller. In other words, changes that you make to the Microsoft.ActiveDirectory.WebServices.exe.config file on a domain controller in a given domain or forest do not replicate to other domain controllers in this domain or forest.

The following table lists the names, default values, and descriptions of the ADWS configuration parameters that determine how the ADWS service handles the traffic that is generated by administrators who are managing AD DS and AD LDS instances and Active Directory Database Mounting Tool instances by using the Active Directory module or Active Directory Administrative Center.

How should I prepare to deploy ADWS?

The ADWS service is installed automatically when you add the AD DS or AD LDS server roles to your Windows Server 2008 R2 server. The ADWS service is configured to run if you make this Windows Server 2008 R2 server a domain controller by running Dcpromo.exe or if you create an AD LDS instance on this Windows Server 2008 R2 server.

What does the Active Directory Management Gateway Service do?

Active Directory Management Gateway Service runs as the Windows Server 2008 R2 ADWS service and provides the same functionality.

You can download and install the Active Directory Management Gateway Service on servers and domain controllers running the following operating systems:

- Windows Server® 2003 R2 with Service Pack 2 (SP2)
- Windows Server 2003 SP2
- Windows Server 2008
- Windows Server 2008 SP2

After it is installed on any of these operating systems, Active Directory Management Gateway Service provides the same functionality to domain controllers that are running Windows Server® 2003 R2 with SP2, Windows Server 2003 SP2, Windows Server 2008, and Windows Server 2008 SP2 operating systems as ADWS provides for domain controllers that are running Windows Server 2008 R2 operating system.

What's New in AD DS: Authentication Mechanism Assurance

What are the major changes?

Authentication mechanism assurance is a new feature in Active Directory Domain Services (AD DS) in Windows Server 2008 R2. This feature is not enabled by default. It requires a domain functional level of Windows Server 2008 R2 as well as a certificate-based authentication infrastructure and additional configuration.

What does authentication mechanism assurance do?

When you enable it, authentication mechanism assurance adds an administrator-designated, universal group membership to a user's access token when the user's credentials are authenticated during logon with a certificate-based logon method. This makes it possible for network resource administrators to control access to resources, such as files, folders, and printers, based on whether the user logs on with a certificate-based logon method and the type of certificate that is used for logon. For example, when a user logs on with a smart card, the user's access to resources on the network can be specified as different from what that access would be when the user does not use a smart card (that is, when the user types a user name and password). Without authentication mechanism assurance, there is no distinction in the access token of a user who logs on with certificate-based authentication and a user who logs on with a different method of authentication.

Who will be interested in this feature?

This feature is intended to be used with Active Directory Federation Services (AD FS), custom authorization schemes, or both. Therefore, organizations that have or plan to deploy AD FS or custom authorization schemes will be interested in this feature.

The following groups or people might be interested in these changes:

- Information security administrators or officers
- Enterprise administrators
- Secured resource administrators
- Information security and regulatory compliance auditors
- Chief information officers (CIOs)

Are there any special considerations?

This feature is intended for organizations that use certificate-based authentication methods, such as smart card or token-based authentication systems. Organizations that do not use certificate-based authentication methods will not be able to use authentication mechanism assurance, even if they have Windows Server 2008 R2 domain controllers with their domain functional level set to Windows Server 2008 R2.

What new functionality does this feature provide?

Authentication mechanism assurance makes it possible for access to network resources to be controlled to recognize certificate-based logons using certificates that were issued by specific certificate issuance policies. When a certificate-based logon method (for example, smart-card logon) is used and authentication mechanism assurance is enabled, an additional group membership is added to the user's access token during logon. An administrator links the universal group membership to a specific certificate issuance policy, which is included in the certificate template. Because different certificate issuance policies can be linked to different universal groups, the administrator can use group membership to identify whether a certificate was used during the logon operation. The administrator can also distinguish between different certificates based on the certificate issuance policy object identifier (OID) that corresponds to the certificate issuance policy from which the certificate was issued. Ultimately, authentication mechanism assurance makes it possible for resource administrators to secure resources by using group memberships that recognize that a user was authenticated with a certificate-based authentication method that used a certificate that was issued from a particular certificate issuance policy.

For example, assume a user named Tom has a smart card with a certificate that was issued from a certificate issuance policy named Top Secret. If authentication mechanism assurance is used to map certificates issued from the Top Secret certificate issuance policy to provide membership in a universal group named Top Secret Users, when Tom logs on using his smart card, he receives an additional group membership indicating that he is a member of Top Secret Users. Resource administrators can set permissions on resources so that only members of Top Secret Users are granted access. This means that when Tom logs on using his smart card, he can access resources that grant access to Top Secret Users, but he cannot access those resources when he logs on without using the smart card (for example, by typing a user name and password).

How should I prepare to deploy this feature?

If you want to implement authentication mechanism assurance, the domain functional level has to be increased to Windows Server 2008 R2. You must also have or establish a certificate-based authentication method. The certificates to be used for logon must be distributed from a certificate issuance policy, because it is the certificate issuance policy OID that is linked to a universal security group membership.

What's New in AD DS: Offline Domain Join

What are the major changes?

Offline domain join is a new process that joins computers running Windows® 7 or Windows Server 2008 R2 to a domain in Active Directory Domain Services (AD DS)—without any network connectivity. This process includes a new command-line tool, Djoin.exe, which you can use to complete an offline domain join.

What does offline domain join do?

You can use offline domain join to join computers to a domain without contacting a domain controller over the network. You can join computers to the domain when they first start up after an operating system installation. No additional restart is necessary to complete the domain join. This helps reduce the time and effort required to complete a large-scale computer deployment in places such as datacenters.

For example, an organization might need to deploy many virtual machines within a datacenter. Offine domain join makes it possible for the virtual machines to be joined to the domain when they initially start following the operating system installation. No additional restart is required to complete the domain join. This can significantly reduce the overall time required for wide-scale virtual machine deployments.

A domain join establishes a trust relationship between a computer running a Windows operating system and an Active Directory domain. This operation requires state changes to AD DS and state changes on the computer that is joining the domain. To complete a domain join in the past using previous Windows operating systems, the computer that joined the domain had to be running and it had to have network connectivity to contact a domain controller. Offline domain join provides the following advantages over the previous requirements:

- The Active Directory state changes are completed without any network traffic to the computer.
- The computer state changes are completed without any network traffic to a domain controller.
- Each set of changes can be completed at a different time.

The following sections explain some of the benefits that offline domain join can provide.

Reduced total cost of ownership in datacenters
Offline domain join can reduce the total cost of ownership for computers by reducing the startup time that is required for each server and by increasing the reliability of domain join operations in production environments. Datacenters today commonly have a provisioning server that configures an image and then sends that image to be deployed on a production computer. The production computer is set up, joined to the domain, and restarted. If there are any problems associated with the domain join, such as network connectivity problems or problems associated with necessary servers that are offline, the problems have to be diagnosed and resolved at that time. In this situation, offline domain join helps prevent problems that can arise with the communication between the production computer and a domain controller by configuring the domain join information during the setup for the production computer. The total amount of time to set up each server is reduced by eliminating the additional restart that is required to complete an online domain join.

Improved experience for performing domain joins using an RODC
In Windows Server 2008, there is a mechanism to perform domain join operations against a read-only domain controller (RODC). However, a domain join operation that is performed against an RODC involves the following multiple steps:

1. Precreate the computer account in the directory, and set some additional attributes using scripts.

2. If necessary, modify the Password Replication Policy (PRP) of the RODC to allow the password for the computer that you want to join to the domain to be cached by the RODC.

3. Force replication of the secrets of the computer that is to join to the domain.

4. Communicate the password offline to the computer that is about to join to the domain.

5. Run a custom script that targets the RODC to complete the join.

When you use offline domain join, the steps for performing domain join operations against an RODC are simplified, as follows:

1. Precreate the account in AD DS.

2. Send the relevant state information that the domain-joining computer needs to consume to a text file.

3. The computer consumes the information in the text file and then, when it starts, it is joined to the domain.

Rapid enterprise deployments
By using deployment tools, such as Windows System Image Manager, you can perform an unattended domain join during an operating system installation by providing information that is relevant to the domain join in an Unattend.xml file. Using the same Unattend.xml file, you can supply the information necessary for the computers that run Windows 7 and Windows Server 2008 R2 to perform offline domain join.

The Unattend.xml file for Windows 7 and Windows Server 2008 R2 includes a new section to support offline domain join.

Are there any special considerations?

You can run Djoin.exe only on computers that run Windows 7 or Windows Server 2008 R2. The computer on which you run Djoin.exe to provision computer account data into AD DS must be running Windows 7 or Windows Server 2008 R2. The computer that you want to join to the domain must also run Windows 7 or Windows Server 2008 R2.

By default, the Djoin.exe commands target a domain controller that runs Windows Server 2008 R2. However, you can specify an optional **/downlevel** parameter if you want to target a domain controller that is running a version of Windows Server that is earlier than Windows Server 2008 R2.

To perform an offline domain join, you must have the user rights that are necessary to join workstations to the domain. By default, members of the Domain Admins group have the user rights to join workstations to a domain. If you are not a member of the Domain Admins group, you must either be granted or delegated these user rights.

Is it available in both 32-bit and 64-bit versions?
Djoin.exe is included in both Windows 7 and Windows Server 2008 R2, and it is available in both 32-bit and 64-bit versions. However, the 64-bit-encoded BLOB that results from the provisioning command is architecture independent. Therefore, you can run Djoin.exe on either a 32-bit computer or a 64-bit computer to provision computer account data in AD DS. You can run Djoin.exe again on either a 32-bit computer or a 64-bit computer to request the offline domain join.

Bridgehead Server Selection

In Windows Server 2008 R2, load-balancing was introduced to distribute the workload evenly among bridgehead servers.

In pre–Windows Server 2008 R2 environments, inbound connections from sites typically flooded one domain controller in the hub site with requests. This was the case even if the connections to the hub site were in a load–balanced state.

Consider the following scenario:

- 5 read/write domain controllers (RWDCs) in a hub site, all of which are available bridgeheads
- 50 read-only domain controllers (RODCs), each in its own branch site
- 50 RWDCs, each in its own branch site (101 sites total)
- Site links exist from the hub to each branch site, but no cross-branch site links exist.

For Windows Server 2008 and earlier server operating systems, the initial configuration resembles the following:

- All the branch domain controllers, RWDCs, and RODCs probabilistically load-balance their inbound connections across the 5 hub domain controllers.
- The 5 hub domain controllers do not have much load-balancing. The majority—50 percent or more—of the site's inbound connections from the 50 RWDCs in the branches come to the same hub domain controller.

In Windows Server 2008 R2, the initial configuration resembles the following:

- All the branch domain controllers (RWDCs and RODCs) probabilistically load-balance their inbound connections across the 5 hub domain controllers.
- The 5 hub domain controllers have 100-percent load-balanced, inbound connections to the branches. Each domain controller has 10 connections from the branch RWDCs.

Now, an additional domain controller is added to the hub site, for a total of 6 domain controllers. This domain controller is also an available bridgehead server.

In Windows Server 2008 and earlier server operating systems, the following behavior occurs after the additional bridgehead server is added to the site:

- The RODCs probabilistically load-balance their inbound connections across the 6 hub domain controllers. Approximately one-sixth of the RODCs that were using one of the other hub domain controllers switch to the new domain controller.
- The RWDCs ignore the new hub domain controller. To get the RWDCs to load-balance using the new hub domain controller, you have to delete all the inbound connection objects on the RWDCs and run the knowledge consistency checker (KCC) on all of them again.
- There is no load-balancing of inbound connections to the hub. Even if you deleted all the inbound connections, it still loads one domain controller with more inbound connections than the other domain controllers.

In Windows Server 2008 R2, the following behavior occurs after you add the additional bridgehead server to the site:

- The RODCs and RWDCs probabilistically load-balance their inbound connections across the 6 hub domain controllers. Approximately one-sixth of the RODCs and RWDCs that were using one of the other hub domain controllers switch to the new domain controller.

- The 6 hub domain controllers load-balance the inbound connections to the branches. Four of the hub domain controllers have 8 connections from the branch RWDCs and 2 of the hub domain controllers have 9 connections from the branch RWDCs.

Notes

- The new bridgehead server selection process does not load-balance within one site. That algorithm does not change from previous operating system releases.

- The new bridgehead server selection process does not load-balance the spanning tree. Therefore, if you have 100 domain controllers—all in their own sites—with a totally connected site link set (meaning a link from every site to every site) and all site links have equal cost, there is no load-balancing. The load-balancing previously described is only between two sites.

- The system clock seeds the probabilistic choices. During testing, if you run the KCC simultaneously at all the branch sites, the inbound connection does not load-balance. The inbound connections all choose the same hub domain controller. If you run the KCC at least one second apart, the probabilistic load-balancing works.

- Adding more than one naming context (NC) confuses the scenario, because an already existing connection—even if it is for a different NC—is always used instead a new one. Therefore, in a multidomain scenario, the “pure” load-balancing is mixed with load-balancing from other NCs. This scenario does not always appear to be balanced, but it is within the described parameters of the new load balancing feature.

Chapter 3 – What's New in Distributed File System

Chapter 3

What are the major changes?

Distributed File System (DFS) Namespaces and DFS Replication offer simplified, highly available access to files, load sharing, and WAN-friendly replication. In the Windows Server® 2008 R2 operating system, Microsoft has added a number of features and improvements to existing features.

The following changes to DFS Namespaces are available in Windows Server 2008 R2:

- DFS Management support for enabling access-based enumeration
- Performance counters
- Performance improvements for large namespaces
- DFS Management support to selectively enable namespace root referrals
- Improved Dfsdiag.exe command prompt Help text

The following changes to DFS Replication are available in Windows Server 2008 R2:

- Failover cluster support
- Read-only replicated folders
- Read-only domain controllers have read-only SYSVOL folders
- Additional DFS Replication diagnostic functionality in the Dfsrdiag.exe command-line tool

Who will be interested in this feature?

Administrators of large networks who want to organize and increase the availability of shared folders by creating a namespace and administrators who want to keep folders synchronized between servers in an efficient manner by using DFS Replication will be interested in this feature.

What new functionality does DFS Namespaces provide?

The following changes are available in Windows Server 2008 R2 for DFS Namespaces:

- DFS Management support for enabling access-based enumeration
- Performance counters
- Performance improvements for large namespaces
- DFS Management support to selectively enable namespace root referrals
- Improved Dfsdiag.exe command prompt Help text

DFS Management support for enabling access-based enumeration
Access-based enumeration displays only the files and folders that a user has permissions to access. If a user does not have Read (or equivalent) permissions for a folder, Windows hides the folder from the user's view. For example, if you enable access-based enumeration on a shared folder that contains many users' home directories, users who access the shared folder can see only their personal home directories; other users' folders are hidden from view.

You can enable access-based enumeration in two complementary locations:

- When you enable access-based enumeration on a shared folder by using Share and Storage Management, Windows displays folders and files in the NTFS file system to network users only if they have Read (or equivalent) permissions to the folders and files.

- When you enable access-based enumeration on a namespace by using DFS Management (or the `Dfsutil` command, which is also supported in Windows Server 2008), Windows displays folders in the namespace to network users only if the namespace administrator has given them Read permissions to the DFS folders.

What new functionality does DFS Replication provide?

The following changes are available in Windows Server 2008 R2 for DFS Replication:

- Failover cluster support for DFS Replication

- Read-only replicated folders

- Read-only domain controllers have read-only SYSVOL folders

- Additional DFS Replication diagnostic functionality in the Dfsrdiag.exe command-line tool

Failover cluster support for DFS Replication
DFS Replication in Windows Server 2008 R2 includes the ability to add a failover cluster as a member of a replication group. The DFS Replication service on versions of Windows prior to Windows Server 2008 R2 is not designed to coordinate with a failover cluster, and the service will not fail over to another node.

Read-only replicated folders
A read-only replicated folder is a replicated folder on a particular member in which users cannot add or change files. This is convenient for read-only folders that you want to keep up-to-date with a central server (or servers). For example, you might want to create read-only replicated folders for software installation folders or for folders that contain published reports or documents. Read-only replicated folders are also used by read-only domain controllers (RODCs) to keep the SYSVOL shared folder updated while preventing local changes.

Prior to Windows Server 2008 R2, the only way to simulate a read-only replicated folder was to manually set share permissions and ACLs on the folders to prevent accidental changes or additions, requiring additional administrative effort and increasing the likelihood of mistakes.

Read-only domain controllers have read-only SYSVOL folders
In Windows Server 2008 it is possible to make changes to the SYSVOL folder of a RODC. These changes persist until the DFS Replication service can overwrite the changes with data from a read-write domain controller or from the DFS Replication staging folder.

In Windows Server 2008 R2, the SYSVOL folder on RODCs is a read-only replicated folder. This prevents users or administrators from altering files in the folder.

Additional DFS Replication diagnostic functionality in the Dfsrdiag.exe command-line tool
The Dfsrdiag.exe command-line tool includes three new command-line switches that provide enhanced diagnostic capabilities:

- **Dfsrdiag.exe ReplState**. Provides a summary of the replication status across all connections on the specified replication group member. It initiates a snapshot of the internal state of the DFS Replication service and gathers a list of the updates that are currently being processed (downloaded or served) by the service.

- **Dfsrdiag.exe IdRecord**. Displays the DFS Replication ID record and version for the file or folder that you specify by using its path or its Unique Identifier (UID). The DFS Replication service creates an ID record for every file and folder that it replicates, and you can use the ID record and its version information to determine if a file has replicated properly to a particular member.

- **Dfsrdiag.exe FileHash**. Computes and displays the hash value that is generated by the DFS Replication service for a particular file. The hash value is used to compare two files—if the hash value for two files is identical, so are the files.

  For example, if you use a portable hard drive to copy the contents of a replicated folder to a replication group member before the initial replication, it is often useful to verify whether the files that you copied (for example, the attributes, timestamps, and access control lists (ACLs)) are identical to the version of the files on the authoritative replication group member. If the files are identical, the DFS Replication service doesn't download any portion of the file during replication (except for its metadata, which the service uses to determine that the files are identical).

Which editions include these features?

The following editions of Windows Server 2008 R2 can host DFS namespaces:

- Windows Server 2008 R2 Standard
- Windows Server 2008 R2 Enterprise
- Windows Server 2008 R2 Datacenter
- Windows Server 2008 R2 for Itanium-Based Systems

The following editions of Windows Server 2008 R2 can act as a member of a DFS Replication group:

- Windows Server 2008 R2 Standard
- Windows Server 2008 R2 Enterprise
- Windows Server 2008 R2 Datacenter

Chapter 4 – What's New in DNS

What are the major changes?

Support for Domain Name System Security Extensions (DNSSEC) is introduced in Windows Server® 2008 R2 and Windows® 7. With Windows Server 2008 R2 DNS server, you can now sign and host DNSSEC-signed zones to provide security for your DNS infrastructure.

The following changes are available in DNS server in Windows Server 2008 R2:

- Ability to sign a zone and host signed zones.
- Support for changes to the DNSSEC protocol.
- Support for DNSKEY, RRSIG, NSEC, and DS resource records.

The following changes are available in DNS client in Windows 7:

- Ability to indicate knowledge of DNSSEC in queries.
- Ability to process the DNSKEY, RRSIG, NSEC, and DS resource records.
- Ability to check whether the DNS server with which it communicated has performed validation on the client's behalf.

The DNS client's behavior with respect to DNSSEC is controlled through the Name Resolution Policy Table (NRPT), which stores settings that define the DNS client's behavior. The NRPT is typically managed through Group Policy.

What does DNSSEC do?

DNSSEC is a suite of extensions that add security to the DNS protocol. The core DNSSEC extensions are specified in RFCs 4033, 4034, and 4035 and add origin authority, data integrity, and authenticated denial of existence to DNS. In addition to several new concepts and operations for both the DNS server and the DNS client, DNSSEC introduces four new resource records (DNSKEY, RRSIG, NSEC, and DS) to DNS.

In short, DNSSEC allows for a DNS zone and all the records in the zone to be cryptographically signed. When a DNS server hosting a signed zone receives a query, it returns the digital signatures in addition to the records queried for. A resolver or another server can obtain the public key of the public/private key pair and validate that the responses are authentic and have not been tampered with. In order to do so, the resolver or server must be configured with a trust anchor for the signed zone, or for a parent of the signed zone.

Who will be interested in this feature?

This feature will be of interest to IT professionals who manage Active Directory® Domain Services (AD DS) and DNS, as well as to security administrators. Specifically, this feature will be of interest to all administrators of U.S. federal IT systems who must be compliant with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53.

What new functionality does DNSSEC provide?

The DNSSEC implementation in Windows Server 2008 R2 DNS server provides the ability to sign both file-backed and Active Directory–-integrated zones through an offline zone signing tool. This signed zone will then replicate or zone-transfer to other authoritative DNS servers. When configured with a trust anchor, a DNS server is capable of performing DNSSEC validation on responses received on behalf of the client.

The DNS client in Windows Server 2008 R2 and Windows® 7 is a non-validating security-aware stub resolver. This means that the DNS client will offload the validation responsibilities to its local DNS server, but the client is capable of consuming DNSSEC responses. The DNS client's behavior is controlled by a policy that determines whether the client should check for validation results for names within a given namespace. The client will return the results of the query to the application only if validation has been successfully performed by the server.

Why is this change important?

As DNS security threats become more topical, it is important to realize that securing the DNS is critical to securing enterprise networks and the Internet. DNS is often subject to man-in-the-middle, spoofing, and cache-poisoning attacks that are hard to defend against. DNSSEC is the best available solution that helps protects against these security threats against DNS. DNSSEC will be the technology of choice for enterprises, registrars, and ISPs as they look for ways to secure their DNS deployments.

Are there any dependencies?

Last hop communication refers to the communication between a DNSSEC-enabled client computer running Windows 7 and its local DNS server. We strongly recommend the use of Internet Protocol security (IPsec) to secure last hop communication between the client and the DNS server, but keep the following deployment considerations mind:

- DNSSEC uses Secure Sockets Layer (SSL) to ensure that client-to-server communication is secure. The use of SSL allows the DNS client to check that the server has a certificate that proves its identity as a valid DNS server. This adds an additional level of trust between the client and the server.

- If you have a domain IPsec policy as part of a server and domain isolation deployment, then you must exempt TCP/UDP port 53 traffic (DNS traffic) from the domain IPsec policy. Otherwise, the domain IPsec policy will be used and certificate-based authentication will not be performed. The client will fail the EKU validation and will not trust the DNS server.

DNS Devolution

With devolution, the DNS resolver creates new FQDNs by appending the single-label, unqualified domain name with the parent suffix of the primary DNS suffix name, and the parent of that suffix, and so on, stopping if the name is successfully resolved or at a level determined by devolution settings. Devolution works by removing the left-most label and continuing to get to the parent suffix.

For example, if the primary DNS suffix is *central.contoso.com* and devolution is enabled with a devolution level of two, an application attempting to query the host name *emailsrv7* will attempt to resolve *emailsrv7.central.contoso.com* and *emailsrv7.contoso.com*. If the devolution level is three, an attempt will be made to resolve emailsrv7.central.contoso.com, but not emailsrv7.contoso.com.

Devolution is not enabled in Active Directory domains when the following conditions are true:

1. A global suffix search list is configured using Group Policy.

2. The Append parent suffixes of the primary DNS suffix check box is not selected on the DNS tab in the Advanced TCP/IP Settings for IPv4 or IPv6 Internet Protocol (TCP/IP) Properties of a client computer's network connection. Parent suffixes are obtained by devolution.

What are the major changes?

The DNS client in Windows Server 2008 R2 and Windows 7 introduce the concept of a devolution level, which provides control of the label where devolution will terminate. Previously, the effective devolution level was two. An administrator can now specify the devolution level, allowing for precise control of the organizational boundary in an Active Directory domain when clients attempt to resolve resources within the domain. This update to DNS devolution is also available for previous versions of Microsoft Windows. Changes to the devolution level can affect the ability of client computers to resolve the names of resources in a domain. The following is the new default behavior for DNS devolution:

First, the Forest Root Domain (FRD) and primary DNS suffix of the local computer are determined. Based on this information:

1. If the number of labels in the forest root domain is 1 (single labeled), devolution is not performed.

   Example: The FRD is *contoso* and the primary DNS suffix is *contoso.com*. Devolution is not performed in this case because *contoso* is single-labeled. Previously, the devolution level was two.

2. If the primary DNS suffix is a trailing subset of (ends with) the forest root domain, the devolution level is set to the number of labels in the FRD.

   Example: The FRD is *corp.contoso.com* and the primary DNS suffix is *east.corp.contoso.com*. Devolution level in this case is three because *east.corp.contoso.com* ends with *corp.contoso.com* and the FRD has three labels. Previously, the devolution level was two.

3. If the primary DNS suffix is not a trailing subset of the FRD, devolution is not performed.

   Example: The FRD is *corp.contoso.com* and the primary DNS suffix is *east.contoso.com*. Devolution is not performed in this case because *east.contoso.com* does not end with *corp.contoso.com*. Previously, the devolution level was two.

The following table summarizes the default behavior for devolution after applying the update.

Primary DNS Suffix	FRD: contoso	FRD: contoso.com	FRD: corp.contoso.com	FRD: corp.contoso.net
contoso	OFF (FRD is single-labeled)	OFF (contoso does not end with contoso.com)	OFF (contoso does not end with corp.contoso.com)	OFF (contoso does not end with corp.contoso.net)
contoso.com	OFF (FRD is single-labeled)	Devolution level: 2 (contoso.com ends with contoso.com and FRD has two labels)	OFF (contoso.com does not end with corp.contoso.com)	OFF (contoso.com does not end with corp.contoso.net)
corp.contoso.com	OFF (FRD is single-labeled)	Devolution level: 2 (corp.contoso.com ends with contoso.com and FRD has two labels)	Devolution level: 3 (corp.contoso.com ends with corp.contoso.com and FRD has three labels)	OFF (corp.contoso.com does not end with corp.contoso.net)

corp.contoso.net	OFF (FRD is single-labeled)	OFF (corp.contoso.net does not end with contoso.com)	OFF (corp.contoso.net does not end with corp.contoso.com)	Devolution level: 3 (corp.contoso.net ends with corp.contoso.net and FRD has three labels)

Previously, devolution was done until only two labels in the suffix were left. Now, assuming a contiguous namespace, devolution proceeds down to the FRD name and no further. If DNS resolution is required past the level of the FRD, the following options are available:

1. **Configure a global suffix search list**. When you configure a suffix search list, devolution is disabled and the suffix search list is used instead.

2. **Specify the devolution level**. You can configure the devolution level using Group Policy or by configuring the **DomainNameDevolutionLevel** registry key.

DNS Cache Locking

What are the major changes?

Cache locking is a new feature available if your DNS server is running Windows Server 2008 R2. When you enable cache locking, the DNS server will not allow cached records to be overwritten for the duration of the time to live (TTL) value. Cache locking provides for enhanced security against cache poisoning attacks. You can also customize the settings used for cache locking.

What does cache locking do?

When a recursive DNS server responds to a query, it will cache the results obtained so that it can respond quickly if it receives another query requesting the same information. The period of time the DNS server will keep information in its cache is determined by the Time to Live (TTL) value for a resource record. Until the TTL period expires, information in the cache might be overwritten if updated information about that resource record is received. If an attacker successfully overwrites information in the cache, they might be able to redirect traffic on your network to a malicious site.

Who will be interested in this feature?

This feature will be of interest to IT professionals who manage Active Directory® Domain Services (AD DS) and DNS, as well as to security administrators.

Are there any special considerations?

Cache locking is configured as a percent value. For example, if the cache locking value is set to 50, then the DNS server will not overwrite a cached entry for half of the duration of the TTL. By default, the cache locking percent value is 100. This means that cached entries will not be overwritten for the entire duration of the TTL. The cache locking value is stored in the **CacheLockingPercent** registry key. If the registry key is not present, then the DNS server will use the default cache locking value of 100.

DNS Socket Pool

What are the major changes?

A DNS server running Windows Server® 2008 R2, or that has installed security update MS08-037, will use source port randomization to protect against DNS cache poisoning attacks. With source port randomization, the DNS server will randomly pick a source port from a pool of available sockets that it opens when the service starts.

What does Socket Pool do?

Instead of using a predicable source port when issuing queries, the DNS server uses a random port number selected from this pool, known as the socket pool. The socket pool makes cache poisoning attacks more difficult because an attacker must correctly guess the source port of a DNS query in addition to a random transaction ID to successfully execute the attack.

Who will be interested in this feature?

This feature will be of interest to IT professionals who manage Active Directory® Domain Services (AD DS) and DNS, as well as to security administrators.

The default size of the socket pool is 2500. When you configure the socket pool, you can choose a size value from 0 to 10000. The larger the value, the greater protection you will have against DNS spoofing attacks. If you configure a socket pool size of zero, the DNS server will use a single socket for remote DNS queries. If the DNS server is running Windows Server 2008 R2, you can also configure a socket pool exclusion list.

Chapter 5 – What's New in Failover Clusters

What are the major changes?

In Windows Server® 2008 R2 Enterprise and Windows Server® 2008 R2 Datacenter, the changes in failover clusters include the following:

- Improvements to the validation process for a new or existing cluster.
- Improvements in functionality for clustered virtual machines (which run with the Hyper-V feature). These improvements help to increase the uptime and simplify the management of clustered virtual machines.
- The addition of a Windows PowerShell interface.
- Additional options for migrating settings from one cluster to another.

What does a failover cluster do?

A failover cluster is a group of independent computers that work together to increase the availability of applications and services. The clustered servers (called nodes) are connected by physical cables and by software. If one of the cluster nodes fails, another node begins to provide service (a process known as failover). Users experience a minimum of disruptions in service.

Who will be interested in failover clustering?

Failover clusters are used by IT professionals who need to provide high availability for services or applications.

Are there any special considerations?

Microsoft supports a failover cluster solution only if all the hardware components are marked as "Certified for Windows Server 2008 R2." In addition, the complete configuration (servers, network, and storage) must pass all tests in the Validate a Configuration wizard, which is included in the Failover Cluster Manager snap-in.

Note that this policy differs from the support policy for server clusters in Windows Server 2003, which required the entire cluster solution to be listed in the Windows Server Catalog under Cluster Solutions.

What new functionality does failover clustering provide?

- **Windows PowerShell cmdlets for failover clusters**. Windows PowerShell is a new command-line shell and scripting technology that uses consistent syntax and naming patterns across the roles and features in Windows Server 2008 R2. The new cmdlets for failover clusters provide powerful ways to script cluster configuration and management tasks. Windows PowerShell cmdlets will eventually replace the **Cluster.exe** command-line interface.

  If you use the Server Core installation option of Windows Server 2008 R2 for your failover cluster, the Windows PowerShell cmdlets for failover clusters simplify the local management of the cluster.

- **Read-only permissions option**. You can assign read-only permission to a user or group who might need to see the cluster but not change the configuration of the cluster.

- **Cluster Shared Volumes**. With Cluster Shared Volumes, the configuration of clustered virtual machines (supported by the Hyper-V feature) is much simpler than before. With Cluster Shared Volumes:

  - You can reduce the number of LUNs (disks) required for your virtual machines, instead of having to manage one LUN per virtual machine. (Previously, the recommended configuration was one LUN per virtual machine, because the LUN was the unit of failover.) Many virtual machines can use a single LUN and can fail over without causing the other virtual machines on the same LUN to also fail over.

  - You can make better use of disk space, because you do not need to place each Virtual Hard Disk (VHD) file on a separate disk with extra free space set aside just for that VHD file. Instead, the free space on a Cluster Shared Volume can be used by any VHD file on that LUN.

  - You can more easily track the paths to VHD files and other files used by virtual machines. You can specify the path names, instead of identifying disks by drive letters (limited to the number of letters in the alphabet) or identifiers called GUIDs (which are hard to use and remember). With Cluster Shared Volumes, the path appears to be on the system drive of the node, under the **\ClusterStorage** folder. However, this path is the same when viewed from any node in the cluster.

  - If you use a few Cluster Shared Volumes to create a configuration that supports many clustered virtual machines, you can perform validation more quickly than you could with a configuration that uses many LUNs to support many clustered virtual machines. With fewer LUNs, validation runs more quickly. (You perform validation by running the Validate a Configuration Wizard in the snap-in for failover clusters.)

  - There are no special hardware requirements beyond what is already required for storage in a failover cluster (although Cluster Shared Volumes require NTFS).

  - Resiliency is increased, because the cluster can respond correctly even if connectivity between one node and the SAN is interrupted, or part of a network is down. The cluster will re-route the Cluster Shared Volumes traffic through an intact part of the SAN or network.

What existing functionality is changing?

The following list briefly summarizes the improvements in failover clusters:

- **Additional tests in cluster validation**. With the additional tests built into the Cluster Validation Wizard in the failover cluster snap-in, you can fine-tune your cluster configuration, track the configuration, and identify potential cluster configuration issues before they cause downtime.

- **Support for additional clustered services**. In addition to the services and applications you could previously configure in a cluster, you can now cluster Distributed File System (DFS) Replication member servers and a Remote Desktop Connection Broker (formerly Terminal Services Session Broker).

- **Additional options for migrating settings from one cluster to another**. The Migration Wizard built into the failover cluster snap-in can migrate settings from clusters running Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2, not just from clusters running Windows Server 2003 as was previously the case. The wizard can also migrate the settings for additional types of resources and resource groups.

- **Options for moving a virtual machine to another node with little or no interruption for clients**. Windows Server 2008 R2 includes live migration, an option for moving a virtual machine to another node in a way that usually leaves the clients connected to the virtual machine. It also includes quick migration and moving of virtual machines, which are options similar to what was available in clusters running Windows Server 2008.

Additional tests in cluster validation
The cluster validation wizard previously included tests that helped you test a set of servers, their networks, and the attached storage before you brought them together in a cluster. The tests were also useful for re-testing a cluster after you made a change, for example, a change to the storage configuration. These tests continue to be available, with an additional set of tests. The new tests are called the **Cluster Configuration** tests, and they help you to check settings that are specified within the cluster, such as the settings that affect how the cluster communicates across the available networks. These tests analyze your current configuration down to the private properties of clustered resources to see if best practices are employed. You can also use the **Cluster Configuration** tests to review and archive the configurations of your clustered services and applications (including settings for the resources within each clustered service or application).

With these tests, you can fine-tune your cluster configuration, track the configuration, and identify potential cluster configuration issues before they cause downtime. This can help you optimize your configuration and compare it against the best practices that you have identified for your organization.

Support for additional clustered services
In addition to the services and applications you could previously configure in a failover cluster, you can now configure the following:

- **Remote Desktop Connection Broker** (formerly Terminal Services Session Broker): Remote Desktop Connection Broker supports session load balancing and session reconnection in a load-balanced remote desktop server farm. RD Connection Broker is also used to provide users access to RemoteApp programs and virtual desktops through RemoteApp and Desktop Connection.

- **DFS Replication**: DFS Replication is an efficient, multiple-master replication engine that you can use to keep folders synchronized between servers across limited bandwidth network connections. You can cluster any member server in the replication group.

Additional options for migrating settings from one cluster to another
The Migration Wizard built into the failover cluster snap-in can migrate settings from clusters running Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2, not just from a cluster running Windows Server 2003 as was previously the case. As before, the wizard can migrate settings from the following resource groups:

- File server
- Dynamic Host Configuration Protocol (DHCP)
- Generic Application
- Generic Script
- Generic Service
- WINS Server

In Windows Server 2008 R2, the Migration Wizard can also migrate settings from the following resource groups:

- Distributed File System Namespace (DFS-N)
- Distributed Transaction Coordinator (DTC)

- Internet Storage Name Service (iSNS) Server
- Message Queuing (also called MSMQ)
- Network File System (NFS)
- Other Server (client access point and storage only)
- Remote Desktop Connection Broker

Note that other migration processes exist for additional clustered servers, such as clustered print servers.

Options for moving a virtual machine to another node with little or no interruption for clients
Failover clusters in Windows Server 2008 R2 provide multiple ways to move a virtual machine from one cluster node to another:

- **Live migration**: When you initiate live migration, the cluster copies the memory being used by the virtual machine from the current node to another node, so that when the transition to the other node actually takes place, the memory and state information is already in place for the virtual machine. The transition is usually fast enough that a client using the virtual machine does not lose the network connection. If you are using Cluster Shared Volumes, live migration is almost instantaneous, because no transfer of disk ownership is needed.

  A live migration can be used for planned maintenance but not for an unplanned failover. On a given server running Hyper-V, only one live migration (to or from the server) can be in progress at a given time. For example, if you have a four-node cluster, up to two live migrations can occur simultaneously if each live migration involves different nodes.

- **Quick migration**: When you initiate quick migration, the cluster copies the memory being used by the virtual machine to a disk in storage, so that when the transition to another node actually takes place, the memory and state information needed by the virtual machine can quickly be read from the disk by the node that is taking over ownership.

  A quick migration can be used for planned maintenance but not for an unplanned failover. You can use quick migration to move multiple virtual machines simultaneously.

- **Moving**: When you initiate a move, the cluster prepares to take the virtual machine offline by performing an action that you have specified in the cluster configuration for the virtual machine resource:

  - **Save** (the default) saves the state of the virtual machine, so that the state can be restored when bringing the virtual machine back online.
  - **Shut down** performs an orderly shutdown of the operating system (waiting for all processes to close) on the virtual machine before taking the virtual machine offline.
  - **Shut down (forced)** shuts down the operating system on the virtual machine without waiting for slower processes to finish, and then takes the virtual machine offline.
  - **Turn off** is like turning off the power to the virtual machine, which means that data loss may occur.

- The setting that you specify for the offline action does not affect live migration, quick migration, or unplanned failover. It affects only moving (or taking the resource offline through the action of Windows PowerShell or an application).

Chapter 6 – What's New in Group Policy

What are the major changes?

The following changes are available in Windows Server® 2008 R2 and in Windows® 7 with Remote Server Administration Tools (RSAT):

- Windows PowerShell Cmdlets for Group Policy: Ability to manage Group Policy from the Windows PowerShell™ command line and to run PowerShell scripts during logon and startup
- Group Policy Preferences: Additional types of preference items
- Starter Group Policy Objects: Improvements to Starter GPOs
- Administrative Template Functionality: Improved user interface
- Administrative Template Settings: New and changed policy settings

What does Group Policy do?

Group Policy provides an infrastructure for centralized configuration management of the operating system and applications that run on the operating system.

Who will be interested in this feature?

The following groups might be interested in these changes:

- IT professionals who have to manage users and computers in a domain environment
- Dedicated Group Policy administrators
- IT generalists
- Support personnel

Are there any special considerations?

You can manage local and domain Group Policy by using domain-based versions of Windows Server 2008 R2. Although the Group Policy Management Console (GPMC) is distributed with Windows Server 2008 R2, you must install Group Policy Management as a feature through Server Manager.

You can also manage local and domain Group Policy by using Windows 7. For managing local Group Policy, the Group Policy Object Editor has been replaced by the Local Group Policy Editor. To manage domain Group Policy, you must first install the GPMC. The GPMC is included with RSAT, which is available for download:

- Windows Server 2008 R2 Remote Server Administration Tools for Windows 7
- Windows Server 2008 Remote Server Administration Tools for Windows Vista with SP1

RSAT enables IT administrators to remotely manage roles and features in Windows Server 2008 R2 from a computer that is running Windows 7. RSAT includes support for the remote management of computers that are running either a Server Core installation or the full installation option of Windows Server 2008 R2. The functionality RSAT provides is similar to Windows Server 2003 Administration Tools Pack.

Installing RSAT does not automatically install the GPMC. To install the GPMC after you install RSAT, click **Programs** in **Control Panel**, click **Turn Windows features on or off**, expand **Remote Server Administration Tools**, expand **Feature Administration Tools**, and select the **Feature Administration Tools** and **Group Policy Management Tools** check boxes.

Which editions include this feature?

Group Policy is available in all editions of Windows Server 2008 R2 and Windows 7. Both local and domain-based Group Policy can be managed by using any version of Windows Server 2008 R2 and any version of Windows 7 that supports RSAT.

Does it function differently in some editions?

Without RSAT, only local Group Policy can be managed using Windows 7. With RSAT, both local and domain-based Group Policy can be managed using any edition of Windows 7 that supports RSAT.

Windows PowerShell Cmdlets for Group Policy

What do the Windows PowerShell Group Policy cmdlets do?

Windows PowerShell is a Windows command-line shell and scripting language that you can use to automate many of the same tasks that you perform in the user interface by using the Group Policy Management Console (GPMC). To help you perform these tasks, Group Policy in Windows Server 2008 R2 provides more than 25 cmdlets. Each cmdlet is a simple, single-function command-line tool.

You can use the Group Policy cmdlets to perform the following tasks for domain-based Group Policy objects (GPOs):

- Maintaining GPOs: GPO creation, removal, backup, and import.
- Associating GPOs with Active Directory® containers: Group Policy link creation, update, and removal.
- Setting inheritance flags and permissions on Active Directory organizational units (OUs) and domains.
- Configuring registry-based policy settings and Group Policy Preferences Registry settings: Update, retrieval, and removal.
- Creating and editing Starter GPOs.

Are there any special considerations?

To use the Windows PowerShell Group Policy cmdlets, you must be running either Windows Server 2008 R2 on a domain controller or on a member server that has the GPMC installed, or Windows 7 with Remote Server Administration Tools (RSAT) installed. RSAT includes the GPMC and its cmdlets.

You must also use the **Import-Module grouppolicy** command to import the Group Policy module before you use the cmdlets at the beginning of every script that uses them and at the beginning of every Windows PowerShell session.

What policy settings have been added or changed?

New policy settings now enable you to specify whether Windows PowerShell scripts run before non-Windows PowerShell scripts during user computer startup and shutdown, and user logon and logoff. By default, Windows PowerShell scripts run after non-Windows PowerShell scripts.

Group Policy settings

Setting name	Location	Default value	Possible values
Run Windows PowerShell scripts first at computer startup, shutdown	Computer Configuration\Policies\Administrative Templates\System\Scripts\	Not Configured (Windows PowerShell scripts run after non-Windows PowerShell scripts)	Not Configured, Enabled, Disabled **Note** This policy setting determines the order in which computer startup and shutdown scripts are run within all applicable GPOs. You can override this policy setting for specific script types in a specific GPO by configuring the following policy settings for the GPO: **Computer Configuration\Policies\Windows Settings\Scripts (Startup/Shutdown)\Startup** and **Computer Configuration\Policies\Windows Settings\Scripts (Startup/Shutdown)\Shutdown**.
Run Windows PowerShell scripts first at user logon, logoff	Computer Configuration\Policies\Administrative Templates\System\Scripts\	Not Configured (Windows PowerShell scripts run after non-Windows PowerShell scripts)	Not Configured, Enabled, Disabled **Note** This policy setting determines the order in which user logon and logoff scripts are run within all applicable GPOs. You can override this policy setting for specific script types in a specific GPO by configuring the following policy settings for the GPO: **User Configuration\Policies\Windows Settings\Scripts (Logon/Logoff)\Logon** and **User Configuration\Policies\Windows Settings\Scripts (Logon/Logoff)\Logoff**.
Run Windows PowerShell scripts first at user logon, logoff	User Configuration\Policies\Administrative Templates\System\Scripts\	Not Configured (Windows PowerShell scripts run after non-Windows PowerShell scripts)	Not Configured, Enabled, Disabled **Note** This policy setting determines the order in which user logon and logoff scripts are run within all applicable GPOs. You can override this policy setting for specific script types in a specific GPO by configuring the following policy settings for the GPO: **User**

			Configuration\Policies\Windows Settings\Scripts (Logon/Logoff)\Logon and **User Configuration\Policies\Windows Settings\Scripts (Logon/Logoff)\Logoff**.
Startup (**PowerShell Scripts** tab)	Computer Configuration\Policies\Windows Settings\Scripts (Startup/Shutdown)\	Not Configured	Not Configured, Run Windows PowerShell scripts first, Run Windows PowerShell scripts last
Shutdown (**PowerShell Scripts** tab)	Computer Configuration\Policies\Windows Settings\Scripts (Startup/Shutdown)\	Not Configured	Not Configured, Run Windows PowerShell scripts first, Run Windows PowerShell scripts last
Logon (**PowerShell Scripts** tab)	User Configuration\Policies\Windows Settings\Scripts (Logon/Logoff)\	Not Configured	Not Configured, Run Windows PowerShell scripts first, Run Windows PowerShell scripts last
Logoff (**PowerShell Scripts** tab)	User Configuration\Policies\Windows Settings\Scripts (Logon/Logoff)\	Not Configured	Not Configured, Run Windows PowerShell scripts first, Run Windows PowerShell scripts last

Group Policy Preferences

What are the major changes?

The following new types of preference items can be managed by using Windows Server 2008 R2 and Windows 7 with Remote Server Administration Tools (RSAT). The client-side extensions for these new types of preference items are included in Windows Server 2008 R2 and Windows 7:

- Power Plan (Windows Vista and later) preference items
- Scheduled Task (Windows Vista and later) preference items
- Immediate Task (Windows Vista and later) preference items
- Internet Explorer 8 preference items

What do Group Policy Preferences do?

Group Policy Preferences let you manage drive mappings, registry settings, local users and groups, services, files, and folders without the need to learn a scripting language. You can use preference items to reduce scripting and the number of custom system images needed, standardize management, and help secure your networks. By using preference item-level targeting, you can streamline desktop management by reducing the number of Group Policy objects needed.

What new functionality does this feature provide?

Windows Server 2008 R2 and Windows 7 with RSAT improve several preference extensions with the addition of new types of preference items, providing support for power plans; scheduled tasks and immediate tasks for Windows 7, Windows Server 2008, and Windows Vista; and Windows Internet Explorer 8.

Power Plan (Windows Vista and later) preference items
Windows Server 2008 R2 and Windows 7 with RSAT improve the Power Options preference extension with the addition of Power Plan (Windows Vista and later) preference items.

Why is this change important?
You can use Power Plan preference items to configure default sleep and display options for managing power consumption for computers, reducing power consumption and benefitting the environment. With Power Plan preference items, you can let users make changes to those default options. Although you can also manage power options by using enforced policy settings, some user roles (such as mobile users) might need the flexibility to change those settings on their own.

The user interface for Power Plan preference items resembles that for advanced power settings in **Power Options** in **Control Panel**. This similarity makes the functionality easier to learn. As with any other type of preference item, you can use preference item-level targeting to restrict the computers and users to which a Power Plan preference item is applied.

Are there any dependencies?
Power Plan preference items can only be used to manage power consumption for computers that are running Windows 7, Windows Server 2008, and Windows Vista. For computers that are running Windows XP or Windows Server 2003, use Power Options (Windows XP) preference items and Power Scheme (Windows XP) preference items instead.

Scheduled Task (Windows Vista and later) preference items
Windows Server 2008 R2 and Windows 7 with RSAT improve the Scheduled Tasks preference extension with the addition of Scheduled Task (Windows Vista and later) preference items.

Why is this change important?
You can use Scheduled Task (Windows Vista and later) preference items to create, replace, update, and delete tasks and their associated properties. Although you can still use Scheduled Task preference items to manage tasks for Windows 7, Windows Server 2008, and Windows Vista, Scheduled Task (Windows Vista and later) preference items provide a user interface similar to the Task Scheduler in Windows 7, Windows Server 2008, and Windows Vista, together with the options that it provides. As with any other type of preference item, you can use preference item-level targeting to restrict the computers and users to which a Scheduled Task preference item is applied.

Are there any dependencies?
Scheduled Task (Windows Vista and later) preference items can only be used to manage tasks for computers that are running Windows 7, Windows Server 2008, and Windows Vista. For computers that are running Windows XP or Windows Server 2003, use Scheduled Task preference items instead.

Immediate Task (Windows Vista and later) preference items
Windows Server 2008 R2 and Windows 7 with RSAT improve the Scheduled Tasks preference extension with the addition of Immediate Task (Windows Vista and later) preference items.

Why is this change important?
You can use Immediate Task (Windows Vista and later) preference items to create tasks to be run immediately upon the refresh of Group Policy—and then removed. Previously, Immediate Task preference items were not supported for Windows Server 2008 and Windows Vista. Immediate Task (Windows Vista and later) preference items provide an intuitive user interface similar to the Task Scheduler in Windows 7, Windows Server 2008, and Windows Vista, together with the options that it provides. As with any other type of preference item, you can use preference item-level targeting to restrict the computers and users to which an Immediate Task preference item is applied.

Are there any dependencies?
Immediate Task (Windows Vista and later) preference items can only be used to manage tasks for computers that are running Windows 7, Windows Server 2008, and Windows Vista. For computers that are running Windows XP or Windows Server 2003, use Immediate Task (Windows XP) preference items instead.

Internet Explorer 8 preference items
Windows Server 2008 R2 and Windows 7 with RSAT improve the Internet Settings preference extension with the addition of Internet Explorer 8 preference items.

Why is this change important?
You can use Internet Explorer 8 preference items to update Internet options for Internet Explorer 8. As with any other type of preference item, you can use preference item-level targeting to restrict the computers and users to which an Immediate Task preference item is applied.

What works differently?
Internet Explorer 8 and Internet Explorer 7 have different default settings, so that the corresponding types of preference items have different default settings as well.

Are there any dependencies?
Internet Explorer 8 preference items can only be used to manage Internet options for Internet Explorer 8. To manage Internet options for earlier versions of Internet Explorer, use Internet Explorer 7 preference items or Internet Explorer 5 and 6 preference items.

Starter Group Policy Objects

What are the major changes?

System Starter Group Policy objects (GPOs) for the following scenarios are available in Windows Server 2008 R2 and Windows 7 with Remote Server Administration Tools (RSAT):

- Windows Vista Enterprise Client (EC)
- Windows Vista Specialized Security Limited Functionality (SSLF) Client
- Windows XP Service Pack 2 (SP2) EC
- Windows XP SP2 SSLF Client

What do System Starter GPOs do?

System Starter GPOs are read-only Starter GPOs that provide a baseline of settings for a specific scenario. Like Starter GPOs, System Starter GPOs derive from a GPO, let you store a collection of Administrative template policy settings in a single object, and can be imported.

What new functionality does this feature provide?

System Starter GPOs are included as part of Windows Server 2008 R2 and Windows 7 with RSAT and do not have to be downloaded and installed separately.

Why is this change important?
The System Starter GPOs included with Windows Server 2008 R2 and Windows 7 with RSAT provide recommended Group Policy settings for the following scenarios described in either the Windows Vista Security Guide or the Windows XP Security Guide:

- The computer and user Group Policy settings that are recommended for the Windows Vista EC client environment are contained in the Windows Vista EC Computer and Windows Vista EC User System Starter GPOs.
- The computer and user Group Policy settings that are recommended for the Windows Vista SSLF client environment are contained in the Windows Vista SSLF Computer and Windows Vista SSLF User System Starter GPOs.
- The computer and user Group Policy settings that are recommended for the Windows XP SP2 EC environment are contained in the Windows XP SP2 EC Computer and Windows XP SP2 EC User System Starter GPOs.
- The computer and user Group Policy settings that are recommended for the Windows XP SP2 SSLF client environment are contained in the Windows XP SP2 SSLF Computer and Windows XP SP2 SSLF User System Starter GPOs.

What works differently?
You no longer have to download these System Starter GPOs because they are included in Windows Server 2008 R2 and Windows 7 with RSAT.

Administrative Template Settings

What are the major changes?

The following changes are available in Windows Server 2008 R2 and Windows 7 with Remote Server Administration Tools (RSAT):

- Improved user interface
- Support for multi-string registry and QWORD value types

What do Administrative templates do?

Administrative templates (.ADMX files) are registry-based policy settings that appear under the Administrative Templates node of both the Computer and User Configuration nodes. This hierarchy is created when the Group Policy Management Console reads XML-based Administrative template files.

What new functionality does this feature provide?

Administrative templates now provide an improved user interface and support for the multi-string (REG_MULTI_SZ) value and QWORD registry types.

Improved user interface
In previous releases of Windows, the properties dialog box for an Administrative template policy setting included three separate tabs: **Setting** (for enabling or disabling a policy setting and setting additional options), **Explain** (for learning more about a policy setting), and **Comment** (for entering optional information about the policy setting). In Windows Server 2008 R2, these options are available in a single location in the properties dialog box instead of in three separate tabs. This dialog box is now resizable.

Additionally, the **Explain** field, which provides additional information about a policy setting, is now called **Help**.

Why is this change important?
By providing all options required for configuring policy settings in a single location, the improved Administrative templates user interface reduces the administrative time that is required to configure and learn more about policy settings.

Support for multi-string and QWORD registry value types
Administrative templates now provide support for the multi-string (REG_MULTI_SZ) and QWORD registry value types.

Why is this change important?
This change expands Group Policy management options by enabling organizations to use Administrative template policy settings to manage applications that use the REG_MULTI_SZ and QWORD registry value types.

Support for the REG_MULTI_SZ registry value type enables you to perform the following tasks when you configure Administrative template policy settings:

- Enable a policy setting, enter multiple lines of text, and sort entries.
- Edit an existing configured setting, and add new line items.
- Edit an existing configured setting, and edit individual line items.
- Edit an existing configured setting, select one or more entries, and delete selected entries. The entries do not have to be contiguous.

Support for the QWORD registry value type enables you to use Administrative template policy settings to manage 64-bit applications.

What policy settings have been added or changed?

For Group Policy in Windows Server 2008 R2 and Windows 7 with RSAT, more than 300 Administrative template policy settings were added. To learn whether specific policy settings were added or changed for the technologies that are documented in this guide, review the appropriate technology-specific topics.

Chapter 7 – What's New in Hyper-V in Windows Server 2008 R2

Chapter 7

What are the major changes?

The Hyper-V™ role enables you to create and manage a virtualized server computing environment by using a technology that is part of Windows Server® 2008 R2. The improvements to Hyper-V include new live migration functionality, support for dynamic virtual machine storage, and enhancements to processor and networking support.

The following changes are available in Windows Server 2008 R2:

- Live migration
- Dynamic virtual machine storage
- Enhanced processor support
- Enhanced networking support

What does Hyper-V do?

Hyper-V is a role in Windows Server 2008 R2 that provides you with the tools and services you can use to create a virtualized server computing environment. This virtualized environment can be used to address a variety of business goals aimed at improving efficiency and reducing costs. This type of environment is useful because you can create and manage virtual machines, which allows you to run multiple operating systems on one physical computer and isolate the operating systems from each other.

Who will be interested in this feature?

The Hyper-V role is used by IT professionals who need to create a virtualized server computing environment.

What new functionality does Hyper-V provide?

Improvements to Hyper-V include new live migration functionality.

Live migration
Live migration allows you to transparently move running virtual machines from one node of the failover cluster to another node in the same cluster without a dropped network connection or perceived downtime. Live migration requires the failover clustering role to be added and configured on the servers running Hyper-V. In addition, failover clustering requires shared storage for the cluster nodes. This can include an iSCSI or Fiber-Channel Storage Area Network (SAN). All virtual machines are stored in the shared storage area, and the running virtual machine state is managed by one of the nodes.

On a given server running Hyper-V, only one live migration (to or from the server) can be in progress at a given time. This means that you cannot use live migration to move multiple virtual machines simultaneously.

We recommend using the new Cluster Shared Volumes (CSV) feature of Failover Clustering in Windows Server 2008 R2 with live migration. CSV provides increased reliability when used with live migration and virtual machines, and also provides a single, consistent file namespace so that all servers running Windows Server 2008 R2 see the same storage.

Why is this change important?
Live migration does the following to facilitate greater flexibility and value:

- **Provides better agility.** Datacenters with multiple servers running Hyper-V can move running virtual machines to the best physical computer for performance, scaling, or optimal consolidation without affecting users.

- **Reduces costs.** Datacenters with multiple servers running Hyper-V can service their servers without causing virtual machine downtime or the need to schedule a maintenance window. Datacenters will also be able to reduce power consumption by dynamically increasing consolidation ratios and turning off unused servers during times of lower demand.

- **Increases productivity.** It is possible to keep virtual machines online, even during maintenance, which increases productivity for both users and server administrators.

Are there any dependencies?
Live migration requires the failover clustering role to be added and configured on the servers running Hyper-V.

What existing functionality is changing?

The following list briefly summarizes the improvements to existing functionality in Hyper-V:

- **Dynamic virtual machine storage.** Improvements to virtual machine storage include support for hot plug-in and hot removal of the storage on a SCSI controller of the virtual machine. By supporting the addition or removal of virtual hard disks and physical disks while a virtual machine is running, it is possible to quickly reconfigure virtual machines to meet changing requirements. Hot plug-in and removal of storage requires the installation of Hyper-V integration services (included in Windows Server 2008 R2) on the guest operating system.

- **Enhanced processor support.** You can now have up to 64 physical processor cores. The increased processor support makes it possible to run even more demanding workloads on a single host. In addition, there is support for Second-Level Address Translation (SLAT) and CPU Core Parking. CPU Core Parking enables Windows and Hyper-V to consolidate processing onto the fewest number of possible processor cores, and suspends inactive processor cores. SLAT adds a second level of paging below the architectural x86/x64 paging tables in x86/x64 processors. It provides an indirection layer from virtual machine memory access to the physical memory access. In virtualization scenarios, hardware-based SLAT support improves performance. On Itanium-based processors, this is called Extended Page Tables (EPT), and on AMD-based processors, it is called Nested Page Tables (NPT).

- **Enhanced networking support.** Support for jumbo frames, which was previously available in nonvirtual environments, has been extended to be available on virtual machines. This feature enables virtual machines to use jumbo frames up to 9,014 bytes in size, if the underlying physical network supports it.

Chapter 8 – What's New in Microsoft iSCSI Initiator

What are the major changes?

The following changes are available in Windows Server® 2008 R2:

- User interface enhancement and redesign

  The iSCSI Initiator user interface has been redesigned to allow easier access to the most commonly used settings. Additionally, the iSCSI control panel is included in Server Core installations of Windows Server 2008 R2, which enables administrators to configure iSCSI connections through the more familiar user interface in addition to the command-line interface.

  New to the iSCSI Initiator user interface is the Quick Connect feature, which allows one-click connections to storage devices that do not require advanced settings, such as the use of Internet Protocol security (IPsec) and Challenge Handshake Authentication Protocol (CHAP) authentication. You can use Quick Connect as a one-step method to perform discovery, logon, and to make the target location a favorite target.

  Also new to the iSCSI Initiator user interface is the Configuration tab, which allows you to configure iSCSI Initiator for use with CHAP or IPsec, and to generate a configuration report of all connected targets and devices on the system.

- iSCSI digest offload support

  iSCSI Initiator CRC (header and data digests) are offloaded by using a new, industry-standard CPU instruction set. This provides transparent interoperability for all NICs without requiring changes to networking drivers. This helps to decrease CPU utilization, which is important for routed networks. The digest offload support is auto-detected and does not require configuration.

- iSCSI boot support for up to 32 paths at boot time

  Supporting redundant boot paths is an important consideration for IT managers when planning server implementations. Administrators who implement Windows Server 2008 R2 in 24/7 environments require end-to-end redundancy of all components within the system. This includes components within the physical server chassis as well as resiliency from failures in paths to external storage boot and data volumes. In the case of servers booting from external storage devices, just having one additional redundant path does not offer the level of redundancy needed to protect against network component failures or outages.

  Centralizing storage within an external storage chassis enables resilience to hard drive failures and reduces maintenance associated with hard drive replacement. This is especially important for blade server form factors to reduce power and cooling requirements and enable higher density.

Chapter 9 – What's New in Microsoft Multipath I/O

What are the major changes?

The following changes to MPIO are available in Windows Server® 2008 R2:

- MPIO health reporting

  The improved MPIO health model enables IT administrators to more efficiently diagnose and gather information about path health by capturing statistical information that can be reviewed in real time or collected over time for trend analysis. This feature calculates how long paths are down, and it detects inconsistent failovers. MPIO health reporting uses a collection of statistics that are provided through Windows® Management Instrumentation (WMI) classes. It enables quicker root-cause diagnosis for a failover issue on a server that is connected to external storage through multiple paths.

- Enhanced configuration of MPIO load-balance policies

  You can display and configure load-balance policy settings from the command line by using the MPCLAIM utility. This utility makes configuration of MPIO easier, including scripting the new Least Blocks MPIO load balance policy, and MPCLAIM enhancements that allow you to more easily script the configuration of MPIO. It also gives you the ability to configure load balance policies per disk from the command line, or configure global policies that will be applied to all new MPIO disks.

- MPIO configuration reporting

  The MPIO configuration report can be saved as a text file, which makes it easier to show important information such as the Device Specific Module (DSM) file that is in use for a specific device, the number of paths, and the paths' states. You can review the text file for troubleshooting or comparison purposes at a later time.

- MPIO datacenter automation

  MPIO datacenter automation allows IT administrators to configure MPIO settings prior to connecting a storage device. To minimize the configuration that is needed after the storage device is connected, you can preconfigure settings such as the default load-balance policy.

Chapter 10 – What's New in Network Access Protection

Chapter 10

What are the major changes?

Network Access Protection (NAP) provides the following new feature in Windows Server® 2008 R2:

- **Multi-configuration SHV.** This feature targets both the cost of deployment and ownership of NAP servers by allowing you to specify multiple configurations of a system health validator (SHV). When you configure a health policy, you can select one of these SHV configurations. When you configure a network policy for health evaluation, you select a specific health policy. Therefore, different network policies can specify different sets of health requirements based on a specific configuration of the SHV. For example, you can create a network policy that specifies that intranet-connected computers must have antivirus software enabled and a different network policy that specifies that VPN-connected computers must have their antivirus software enabled and signature file up-to-date.

NAP provides the following new feature in Windows® 7:

- **NAP client user interface improvements.** After collecting feedback from end-user interaction with NAP in Microsoft and partner deployments, the end-user experience has been improved by integrating the NAP client user interface into the Action Center on computers running Windows 7.

Who will be interested in these features?

Network administrators, system administrators, and network architects that design and manage a NAP deployment will be interested in these features.

Are there any special considerations?

Following are special considerations for using new features with NAP:

- To use multi-configuration SHVs, NAP health policy servers must be running a Windows Server 2008 R2 operating system.
- Multi-configuration SHVs are only available for SHVs that support this feature, for example the Windows Security Health Validator (WSHV).
- To use NAP client user interface improvements, client computers must be running a Windows 7 operating system.

What new functionality do these features provide?

These features provide greater flexibility and simplicity for administrators that are managing a NAP infrastructure. The following sections describe how you can use these improvements.

Multi-configuration SHV
SHVs define configuration requirements for computers that attempt to connect to your network. For example, the WSHV can be configured to require that some or all of the following are enabled on NAP client computers:

- **Firewall.** If selected, the client computer must have a firewall that is registered with Windows Security Center and enabled for all network connections.
- **Virus protection.** If selected, the client computer must have an antivirus application installed, registered with Windows Security Center, and turned on.
- **Antivirus is up-to-date.** If selected, the client computer can also be checked to ensure that the antivirus signature file is up-to-date.
- **Spyware protection.** If selected, the client computer must have an antispyware application installed, registered with Windows Security Center, and turned on.
- **Antispyware is up-to-date.** If selected, the client computer can also be checked to ensure that the antispyware signature file is up-to-date.
- **Automatic updating.** If selected, the client computer must be configured to check for updates from Windows Update. You can choose whether to download and install them.
- **Security update protection.** If selected, the client computer must have security updates installed based on one of four security severity ratings in the Microsoft Security Response Center (MSRC). The client must also check for these updates by using a specified time interval. You can use choose to use Windows Server Update Services (WSUS), Windows Update, or both to obtain security updates.

To ensure that NAP client computers meet these requirements, you must configure WSHV settings, enable WSHV in a health policy, and then add the health policy condition to a network policy.

When an SHV supports the multi-configuration SHV feature, different settings can be stored in multiple SHV configuration profiles. When you configure a health policy, you can choose which SHV will be used, and custom settings for the SHV if these have been configured. For example, using this feature you might create the following two health policy configurations:

- **Default configuration.** The client computer must have a firewall and Windows Update enabled, antivirus and antispyware applications must be on and up-to-date, and all important security updates must be installed.
- **Trusted configuration.** The client computer must have an antivirus application on and up-to-date.

These settings can then be used to create health policies requiring either default configuration settings or trusted configuration settings. You can create as many unique configuration settings as you require.

Why is this change important?
Previously, it was necessary to use a different NAP health policy server to specify a different set of configurations for the same SHV. With multi-configuration SHV, a single NAP health policy server can be used to deploy multiple configurations of the same SHV.

What works differently?
Multi-configuration SHV affects the procedures used to configure SHVs and health policies. SHV configuration is divided into settings configuration and error codes configuration. If an SHV supports multi-configuration SHV, then additional settings can be created by right-clicking **Settings**, clicking **New**, and then providing a friendly name for the new configuration. If an SHV does not support multi-configuration SHV, you can configure requirements by using the **Default Configuration** settings.

Are there any dependencies?
Multi-configuration SHV is only available if the SHV vendor has designed the SHV to support this feature.

How should I prepare for this change?
Review the NAP policy configuration and settings on all NAP health policy servers on your network to determine how they will be affected by this feature. If you upgrade these servers from Windows Server® 2008 to Windows Server 2008 R2, verify that all SHV settings are correctly migrated to **Default Configuration** settings for all installed SHVs.

NAP client user interface improvements
The end user experience has been enhanced by improving messages the end users sees about NAP and by integrating the NAP client user interface into the Action Center on computers running Windows 7. The Action Center provides a central location to view alerts and take action that can help keep Windows running smoothly.

Why is this change important?
By integrating NAP client notifications with the Action Center, the end user has a comprehensive view of all important security and maintenance settings on their computer that might need attention.

What works differently?
When settings or services on an end user's computer do not meet network requirements, the end user might receive a NAP notification message. These messages have been improved and integrated into the Action Center on computers running Windows 7.

Chapter 11 – What's New in Networking

What are the major changes?

The Windows Server® 2008 R2 and Windows® 7 operating systems include networking enhancements that make it easier for users to get connected and stay connected regardless of their location or type of network. These enhancements also enable IT professionals to meet the needs of their business in a secure, reliable, and flexible way.

New networking features covered in this topic include:

- DirectAccess, which enables users to access an enterprise network without the extra step of initiating a virtual private network (VPN) connection.
- VPN Reconnect, which automatically reestablishes a VPN connection as soon as Internet connectivity is restored, saving users from reentering their credentials and re-creating the VPN connection.
- BranchCache™, which enables updated content from file and Web servers on a wide area network (WAN) to be cached on computers at a local branch office, improving application response time and reducing WAN traffic.
- URL-based Quality of Service (QoS), which enables you to assign a priority level to traffic based on the URL from which the traffic originates.
- Mobile broadband device support, which provides a driver-based model for devices that are used to access a mobile broadband network.
- Multiple active firewall profiles, which enable the firewall rules most appropriate for each network adapter based on the network to which it is connected.
- NDF, Network Tracing, and Netsh Trace, which integrates the Network Diagnostics Framework with Network Tracing and a new Netsh context, Netsh Trace, to simplify and consolidate network connectivity troubleshooting processes.

What does DirectAccess do?

With DirectAccess, domain member computers running Windows 7 Enterprise, Windows 7 Ultimate, or Windows Server 2008 R2 can connect to enterprise network resources whenever they are connected to the Internet. A user on a DirectAccess client computer that is connected to the Internet has virtually the same experience as if connected directly to an organization's private network. Furthermore, DirectAccess allows IT professionals to manage mobile computers outside of the office. Each time a DirectAccess client computer connects to the Internet, before the user logs on, DirectAccess establishes a bi-directional connection to the enterprise network that allows the client computer to stay current with company policies and receive software updates.

Security and performance features of DirectAccess include authentication, encryption, and access control. IT professionals can configure the network resources to which each user can connect, granting unlimited access or allowing access only to specific servers. DirectAccess by default sends only the traffic destined for the enterprise network through the DirectAccess server. DirectAccess clients route Internet traffic directly to the Internet resource. DirectAccess can be configured to send all traffic through the enterprise network.

Are there any special considerations?
The DirectAccess server must be running Windows Server 2008 R2, must be a domain member, must have two physical network adapters installed, and must be configured with two consecutive public Internet Protocol version 4 (IPv4) addresses. DirectAccess clients must be domain members. Use the Add Features Wizard in Server Manager to install the DirectAccess Management Console feature. After installing, use the DirectAccess Management console in Administrative Tools to set up the DirectAccess server and monitor DirectAccess operations.

Infrastructure considerations include the following:

- **Active Directory Domain Services (AD DS).** At least one Active Directory® domain must be deployed. Workgroups are not supported.

- **Group Policy.** Group Policy is recommended for deployment of DirectAccess client, DirectAccess server, and selected server settings.

- **Domain controller.** At least one domain controller must be running Windows Server 2008 or later.

- **Domain Name System (DNS) server.** Windows Server 2008 R2, Windows Server 2008 with the Q958194 hotfix (http://go.microsoft.com/fwlink/?LinkID=159951), Windows Server 2008 SP2 or later, or a third-party DNS server that supports DNS message exchanges over Intra-Site Automatic Tunnel Addressing Protocol (ISATAP).

- **Public key infrastructure (PKI).** A PKI is required to issue certificates for Internet Protocol security (IPsec) peer authentication between DirectAccess clients and servers. This is typically done by deploying computer certificates to DirectAccess clients and servers. External certificates are not required. The DirectAccess server also requires an additional SSL certificate, which must have a certificate revocation list (CRL) distribution point that is reachable via a publicly resolvable fully qualified domain name (FQDN).

- **IPsec.** DirectAccess uses IPsec to provide peer authentication and encryption for communications across the Internet. It is recommended that administrators be familiar with IPsec.

- **IPv6.** Internet Protocol version 6 (IPv6) provides the end-to-end addressing necessary for connectivity to the enterprise network. Organizations that are not yet ready to fully deploy native IPv6 can use the ISATAP IPv6 transition technology to access IPv4 resources on the enterprise network. DirectAccess clients can use the Teredo and 6to4 IPv6 transition technologies to connect across the IPv4 Internet. IPv6 or IPv6 transition technology traffic must be available on the DirectAccess server and allowed to pass through the perimeter network firewall.

What does VPN Reconnect do?

VPN Reconnect is a new feature of Routing and Remote Access Services (RRAS) that provides users with seamless and consistent VPN connectivity, automatically reestablishing a VPN when users temporarily lose their Internet connections. Users who connect using wireless mobile broadband will benefit most from this capability. With VPN Reconnect, Windows 7 automatically reestablishes active VPN connections when Internet connectivity is reestablished. Although the reconnection might take several seconds, it is transparent to users.

VPN Reconnect uses IPsec tunnel-mode with Internet Key Exchange version 2 (IKEv2), which is described in RFC 4306, specifically taking advantage of the IKEv2 mobility and multihoming extension (MOBIKE) described in RFC 4555.

Are there any special considerations?
VPN Reconnect is implemented in the RRAS role service of the Network Policy and Access Services (NPAS) role of a computer running Windows Server 2008 R2. Infrastructure considerations include those for NPAS and RRAS. Client computers must be running Windows 7 to take advantage of VPN Reconnect.

What does BranchCache do?

With BranchCache, content from Web and file servers on the enterprise WAN is stored on the local branch office network to improve response time and reduce WAN traffic. When another client at the same branch requests the same content, the client can access it directly from the local network without obtaining the entire file across the WAN. BranchCache can be set up to operate in either a *distributed cache* mode or a *hosted cache* mode. Distributed cache mode uses a peer-to-peer architecture. Content is cached at the branch office on the client computer that firsts requests it. The client computer subsequently makes the cached content available to other local clients. Hosted cache mode uses a client/server architecture. Content requested by a client at the branch office is subsequently cached to a local server (called the *Hosted Cache server*), where it is made available to other local clients. In either mode, before a client retrieves content, the server where the content originates authorizes access to the content, and content is verified to be current and accurate using a hash mechanism.

Are there any special considerations?
BranchCache supports HTTP, including HTTPS, and Server Message Block (SMB), including signed SMB. Content servers and the hosted cache server must be running Windows Server 2008 R2, and client computers must be running Windows 7.

What does URL-based QoS do?

QoS marks IP packets with a Differentiated Services Code Point (DSCP) number that routers then examine to determine the priority of the packet. If packets are queued at the router, higher priority packets are sent before lower priority packets. With URL-based QoS, IT professionals can prioritize network traffic based on the source URL, in addition to prioritization based on IP address and ports. This gives IT professionals more control over network traffic, ensuring that important Web traffic is processed before less-important traffic, even when that traffic originates at the same server. This can improve performance on busy networks. For example, you can assign Web traffic for critical internal Web sites a higher priority than external Web sites. Similarly non-work-related Web sites that can consume network bandwidth can be assigned a lower priority so that other traffic is not affected.

What does mobile broadband device support do?

The Windows 7 operating system provides a driver-based model for mobile broadband devices. Earlier versions of Windows require users of mobile broadband devices to install third-party software, which is difficult for IT professionals to manage because each mobile broadband device and provider has different software. Users also have to be trained to use the software and must have administrative access to install it, preventing standard users from easily adding a mobile broadband device. Now, users can simply connect a mobile broadband device and immediately begin using it. The interface in Windows 7 is the same regardless of the mobile broadband provider, reducing the need for training and management efforts.

What do multiple active firewall profiles do?

Windows Firewall settings are determined by the profile that you are using. In Windows Vista and Windows Server 2008, only one firewall profile can be active at a time. Therefore, if you have multiple network adapters connected to different network types, you still have only one active profile—the profile providing the most restrictive rules. In Windows Server 2008 R2 and Windows 7, each network adapter applies the firewall profile that is most appropriate for the type of network to which it is connected: Private, Public, or Domain. This means that if you are at a coffee shop with a wireless hotspot and connect to your corporate domain network by using a VPN connection, then the Public profile continues to protect the network traffic that does not go through the tunnel, and the Domain profile protects the network traffic that goes through the tunnel. This also addresses the issue of a network adapter that is not connected to a network. In Windows 7 and Windows Server 2008 R2, this unidentified network will be assigned the Public profile, and other network adapters on the computer will continue to use the profile that is appropriate for the network to which they are attached.

What do NDF, Network Tracing, and Netsh Trace do?

Network Diagnostic Framework (NDF) provides a way for end users, as well as support technicians, and component or application developers, to simplify network troubleshooting by automating many of the common troubleshooting steps and solutions. In Windows® 7, the Network Diagnostic Framework (NDF) and Event Tracing for Windows (ETW) are more closely integrated, which enables diagnostics to log network events and packets in a single file. Collecting all of the needed information in one step provides an efficient method of troubleshooting network connectivity issues. When a user runs Windows Network Diagnostics, a diagnostics session log is automatically created and stored in Action Center/Troubleshooting/View History. Each diagnostic session generates a report with diagnostics results.

In Windows 7 NDF and network tracing, events related to a specific issue are categorized by using activity-ID-based correlation (known as grouping), and then output in an Event Trace Log (ETL) file. Grouping captures all issue-related events across the stack; all related events are grouped together. The result is that you can examine the entire transaction, from end-to-end, as a single collection of events. You can analyze the data in the ETL file by using a number of tools, such as Network Monitor 3.3, Event Viewer, the Netsh trace convert command, or Tracerpt.exe.

Windows 7 includes a new Netsh context, Netsh trace. Netsh trace is also integrated with NDF and Network Tracing, and enables you to perform comprehensive tracing, along with network packet capturing, and filtering. Two key concepts related to Netsh trace are scenarios and providers. A tracing scenario is defined as a collection of selected event providers. Providers are the individual components in the network protocol stack, such as WinSock, TCP/IP, Windows Filtering Platform and Firewall, Wireless LAN Services, or NDIS. You can use commands in the Netsh trace context to enable pre-defined scenarios for troubleshooting specific issues, and to configure specific parameters for a tracing session. For any given scenario, you can view the list of associated providers that will report events when you run a trace session, and view details about specific providers. You can also specify additional providers that are not included in an enabled scenario. Additionally, because it is frequently beneficial to minimize tracing results by limiting irrelevant tracing details, you can apply a variety of Netsh trace filters to reduce the ETL trace file size.

Finally, an additional benefit of NDF and Network Tracing in Windows 7 is that you can use Netsh trace to collect both packet captures and trace events on the client, without requiring installation of Netmon on the computer that your are troubleshooting. Running a tracing session by using Netsh trace correlates and groups packets with related trace events. Because Netmon is only required on the computer that you are using to examine the packets, the user need only copy the file that is collected in Action Center, and then either e-mail it to you or provide it on removable media, such as a USB flash drive.

Chapter 12 – What's New in NTFS

What are the major changes?

Several enhancements to improve performance have been made to the NTFS file system. The following changes are available in Windows® 7 and Windows Server® 2008 R2:

- Delete notification for solid state devices (SSDs) that support T10 Trim
- New opportunistic locks (oplocks) semantics and introduction of oplock keys
- Support for file system metadata defragmenting
- Improvements in Volume Shrink
- Ability to disable short names on a per-volume basis
- Improved concurrency of read requests while flushing
- Native VHD support
- **Chkdsk** performance improvements
- Robocopy performance enhancement
- Local file copy improvements

Who will be interested in this feature?

IT administrators who deploy Windows 7 and Windows Server 2008 R2 will be most interested in these changes to NTFS.

What new functionality does NTFS provide?

This section describes each of the changes that are new to NTFS.

T10 Trim delete notification
In Windows 7 and Windows Server 2008 R2, for storage devices that support T10 Trim, NTFS now sends a delete notification to the device when files are deleted. If a device supports T10 Trim as defined in the ATA protocol's Data Set Management command, NTFS sends the notification when files are deleted and it is safe to erase the storage that backs up those files. This new functionality enables storage devices such as solid state disks (SSDs) to better utilize their storage capability, and it improves their performance.

Oplock semantics
Opportunistic locks (oplocks) provide a mechanism that allows file server client computers that are using the SMB and SMB 2.0 protocols to dynamically alter the buffering strategy for a given file or data stream in a consistent manner. This increases performance and reduces network use. SMB 2.1 brings an important performance enhancement to the protocol in Windows 7 and Windows Server 2008 R2 with the introduction of a new client oplock leasing model. The new leasing model allows greater file and stream handle caching opportunities for an SMB 2.1 client computer, while preserving data integrity. You do not need to make any changes to current applications to take advantage of this capability.

Another important change is the introduction of oplock keys, which apply oplocks on a per-client, rather than per-handle basis. It is becoming more common that single applications open multiple handles to the same file with different access or share modes. Traditionally, the second opening would cause the oplock to revoke or downgrade, thereby impacting the client computer's ability to effectively cache data. The new leasing model helps prevent applications from breaking their oplocks, and it enables the files to take advantage of caching opportunities. This capability helps decrease overall network and disk loads.

Support for file system metadata defragmenting
Prior to Windows 7 and Windows Server 2008 R2, certain file system metadata associated with user data files (for example, reparse point or Encrypting File System (EFS) data) could not be defragmented. Enhancements to the defragment engine enable certain file system metadata to be defragmented. This change helps improve the performance of files with many reparse points and resident files. It can also help enable Volume Shrink to reclaim more space than was previously possible.

Improvements to Volume Shrink
By optimizing the placement of immovable system files, the ability to shrink a volume through the Volume Shrink utility is improved. This results in a greater amount of disk space that can be reclaimed. This enables administrators to avoid moving data off a volume and formatting it, to split the current partition at the free-space boundary.

Ability to disable short names on a per-volume basis
The **shortname** property (a DOS 8.3 naming convention) can now be individually managed on a per-volume basis. Prior versions of Windows only allowed short names to be disabled globally. Also, the command-line utility **Fsutil** has been enhanced with additional **shortname**-related commands. It can now strip short names from a directory, and it keeps a log that contains details of the stripped files and errors that occur. However, after short names have been stripped, there is no automated way to restore them. If the directory structure has changed in any way, there is no guarantee that the short names will be completely restored. Disabling and stripping short names can significantly reduce the time that is required for file creation and directory enumeration in directories with a very large number of files.

Improved concurrency of read requests while flushing
Prior to Windows 7 and Windows Server 2008 R2, if a read request occurred while a file is being flushed (through a call to FlushFileBuffers), the read request would wait until the flush request was completed. To enhance overall concurrency in the system, NTFS now supports a concurrent read request of a file at the same time that cached data is saved to the disk by the flush request.

Native VHD support
Virtual hard disk (VHD) drives are commonly used by virtualization packages, such as Microsoft® Virtual PC, and by Microsoft Hyper-V™-based virtualization systems. Enhancements to the mount and boot mechanisms and additional support across multiple Windows components provide the following capabilities:

- **Instance mobility**: Migrate an operating system instance from one computer to another without having to reconfigure the operating system, the configured roles, or workloads.
- **Multiple-instance VHD management**: Have a single computer maintain multiple instances of operating systems without having to make changes to disk partitioning. Examples of typical usage include easier failover of operating system images and the ability of a server to change workloads.
- **Centralized deployment**: Boot from a single, centralized image, significantly easing the deployment and rollout process.
- **Offline servicing of computer images**: Perform offline servicing of a computer by patching the image, rather than having to bring the VHD online to service it.
- **Backup**: Boot from a backup image through Windows Server Backup.

Chkdsk performance improvements
In Windows Server 2008 R2, enhancements to the command-line tool **Chkdsk** increase the availability of volumes by reducing the amount of time it takes to perform a **Chkdsk** run. **Chkdsk** scales with the amount of available RAM in the system. Running Chkdsk on a server running Windows Server 2008 R2 is significantly faster than on a server running Windows Server 2008 or systems with similar configurations.

Robocopy performance enhancement
The copy utility, Robocopy, has been enhanced to allow for multithreaded copies. This significantly improves remote and high-latency transfer rates by opening multiple threads to perform a concurrent copy operation, which increases the total data throughput.

Local file copy improvements
Optimizations in the memory and cache manager enable improvements in local file copy scenarios. File copy times for small, medium, and large (greater than 8 MB) files have been reduced. The greatest improvement is for medium and large files (depending on the nature of the file set, storage, and memory subsystems).

Chapter 13 – What's New in Offline Files

Chapter 13

What are the major changes?

The major changes to Offline Files for Windows Server 2008 R2 and Windows 7 include significantly improved wide area network (WAN) file access and an improved network file experience for remote users.

Who will be interested in this feature?

The following groups might be interested in these changes:

- Administrators that want to centralize data from client computers for administrative tasks such as backup.
- Network administrators that want to optimize bandwidth usage and enhance the experience of users in branch offices who access files and folders that are hosted by corporate servers located offsite.
- Users that want to continue to access network files if there is a network outage.
- Mobile users that need to access network files while working offline or over slow networks.

What new functionality does Offline Files provide?

New functionality for Offline Files includes the following:

- Fast first logon
- Usually Offline support with Background Sync
- Exclusion List
- Transparent caching

Fast first logon
Fast first logon is a new feature that frees users from waiting while files are copied to the server the first time they log on after a Folder Redirection policy has been applied that redirects the path of a user folder to a network location. It also optimizes network usage on WAN links by synchronizing files as a background task. Prior to Windows 7, after a policy was applied that redirected a user's folder to a network location, the user had to wait while the contents of the folder were moved to the new location. This process could take a considerable amount of time if there was a large amount of data to move and the network was slow. On Windows 7, as long as Offline Files is enabled (it is on by default), the user must wait only for Windows to move the files into the local Offline Files cache. After the files are moved, the user logs on and is free to perform other tasks while Windows synchronizes the locally cached data over the network as a background task.

Usually Offline support with Background Sync
Usually Offline support provides remote and branch office users with faster access to files that are located in a network folder across a slow network connection. Windows 7 enhances this feature by including Background Sync, a feature that synchronizes Offline Files in the background, ensuring that the server is frequently updated with the latest changes. When a client computer's network connection to a server is slow (as configured by the administrator), Offline Files automatically transitions the client computer into an "Offline (slow connection)" mode. The user then works from the local Offline Files cache. On Windows 7, Background Sync runs at regular intervals as

a background task to automatically synchronize and reconcile changes between the client computer and the server. IT administrators can configure synchronization intervals and block out times. With this feature, users no longer must worry about manually synchronizing their data with the server when working offline.

Exclusion List
The Exclusion List feature, reduces synchronization overhead and disk space usage on the server, and speeds up backup and restores operations, by excluding files of certain types from replication across all Folder Redirection clients. Prior to Windows 7, all files in an Offline Files folder were replicated to the server. This often meant that a users' personal files or large files not relevant to the enterprise were replicated to one or more servers, thereby consuming disk space and slowing backup and restore times. On Windows 7, administrators can use the Offline Files Exclusion List feature to prevent files of certain types (for example, MP3 files) from being synchronized. The list of file types is configured by the IT administrator by using Group Policy.

Transparent caching
Transparent caching optimizes bandwidth consumption on WAN links and provides near local read response times for mobile users and branch office workers that are accessing network files and folders that are not explicitly made available offline. Prior to Windows 7, to open a file across a slow network, client computers always retrieved the file from the server, even if the client computer had recently read the file. With Windows 7 transparent caching, the first time a user opens a file in a shared folder, Windows 7 reads the file from the server and then stores it in the Offline Files cache on the local hard disk drive. The subsequent times that a user opens the same file, Windows 7 retrieves the cached file from the hard disk drive instead of reading it from the server. To provide data integrity, Windows 7 always contacts the server to ensure that the cached copy is up to date. The cache is never accessed if the server is unavailable, and updates to the file are always written directly to the server.

Transparent caching is not enabled by default. IT administrators can use a Group Policy setting to enable transparent caching, improve the efficiency of the cache, and configure the amount of hard disk drive space that the cache uses.

What settings have been added or changed?

There are three new Group Policy settings for Offline Files and one setting, "Configure slow-link mode," that has changed. Configure slow-link mode is enabled by default on Windows 7 and Windows Server 2008 R2. It controls when computers running Windows 7 or Windows Server 2008 R2 transition to the slow-link mode. See the Local Group Policy Editor for descriptions of the new settings listed in the following table.

Group Policy settings Setting name	Location	Previous default value (if applicable)	Default value	Possible values
Configure Background Sync	Computer Configuration\Administrative Templates\Network\Offline Files		Enabled	Not configured Enabled Disabled
Exclude files from being cached	Computer Configuration\Administrative Templates\Network\Offline Files		Disabled	Not configured Enabled Disabled
Enable transparent caching	Computer Configuration\Administrative Templates\Network\Offline Files		Disabled	Not configured Enabled Disabled
Configure slow-link mode	Computer Configuration\Administrative Templates\Network\Offline Files	Disabled	Enabled	Not configured Enabled Disabled

Chapter 14 – What's New in Performance and Reliability Monitoring

What are the major changes?

The following changes are available in Windows Server 2008 R2:

- New in Windows® 7 and Windows Server® 2008 R2, **Windows Resource Monitor** is a powerful tool for understanding how your system resources are used by processes and services. In addition to monitoring resource usage in real time, Resource Monitor can help you analyze unresponsive processes, identify which applications are using files, and control processes and services.

- **Reliability Analysis Component** is an in-box agent that provides detailed customer experience information on system usage and reliability. This information is exposed through a Windows Management Instrumentation (WMI) interface, making it available for consumption by Portable Readers Systems. By exposing Reliability Analysis Component through a WMI interface, developers can monitor and analyze their applications, increasing reliability and performance.

  Windows 7 and Windows Server 2008 R2 use the built-in Reliability Analysis Component to calculate a reliability index, which provides information about your overall system usage and stability over time. Reliability Analysis Component also keeps track of any important changes to the system that are likely to have an impact on stability, such as Windows updates and application installations.

  Users of **Reliability Monitor** in Windows Vista® can now find the same reliability statistics as part of the Action Center in the Control Panel. To view reliability statistics, click **Start**, click **Control Panel**, click **System and Security**, click **Action Center**, expand **Maintenance**, and then click **View reliability history**.

What does Resource Monitor do?

Resource Monitor displays per-process and aggregate CPU, memory, disk, and network usage information, in addition to providing details about which processes are using individual file handles and modules. Advanced filtering allows users to isolate the data related to one or more processes (either applications or services), start, stop, pause, and resume services, and close unresponsive applications from the user interface. It also includes a process analysis feature that can help identify deadlocked processes and file locking conflicts so that the user can attempt to resolve the conflict instead of closing an application and potentially losing data.

Chapter 15 – What's New in Print and Document Services

Chapter 15

What are the major changes?

Windows Server® 2008 R2 introduces new functionality and enhancements to Windows printing and scanning services that provides improved performance, increased reliability, and greater flexibility for users.

The following changes are available in Windows Server 2008 R2:

- Print migration enhancements
- Printer driver isolation
- Print administrator delegation
- Print Management snap-in improvements
- Client-Side Rendering (CSR) performance improvements
- XML Paper Specification (XPS) print path improvements
- Location-aware printing
- Distributed Scan Server role service

In addition, there are improvements to the Add Printer Wizard.

What does Print and Document Services do?

In Windows Server 2008 R2, Print and Document Services is a role in Server Manager that enables you to share printers and scanners on a network, set up print servers and scan servers, and centralize network printer and scanner management tasks by using the Print Management and Scan Management Microsoft Management Console (MMC) snap-ins. Print and Document Services replaces and extends the Print Services role in Windows Server® 2008. (The Print Management and Scan Management snap-ins are also available in versions of Windows® 7.)

Who will be interested in this role?

IT professionals who manage print and scan resources in a domain environment will be interested in using this role.

What new functionality does this role provide?

The following enhancements were made to this role in Windows Server 2008 R2.

Print migration enhancements
The Printer Migration Wizard (available through the Print Management snap-in) and the Printbrm.exe command-line tool were introduced in Windows Server 2008 and Windows Vista® to replace the Print Migrator (Printmig) utility. These enable an administrator to easily back up, restore, and migrate print queues, printer settings, printer ports, and language monitors.

Enhancements to the Printer Migration Wizard and Printbrm.exe in Windows Server 2008 R2 provide greater flexibility and better error handling and reporting—for example, you can now restore configuration information for print servers and print queues in a backup. You can also selectively back up specific print processors and print language monitors.

There is also support for print driver isolation setting migration and an option to not restore security settings for print queues during a restore operation.

Printer driver isolation
Prior to Windows Server 2008 R2, the failure of printer driver components has been a main print server support issue—the failure of a printer driver loaded onto the print spooler process would cause the process to fail, which would lead to an outage of the entire printing system. The impact of a spooler failure on a print server is particularly significant because of the number of users and printers that are typically affected.

In Windows Server 2008 R2, you can now configure printer driver components to run in an isolated process separate from the printer spooler process. By isolating the printer driver, you can prevent a faulty printer driver from stopping all print operations on a print server, which results in a significant increase in server reliability.

In addition to the benefit of improving overall printing system stability, this new feature provides a means to isolate new drivers for testing and debugging, and to identify which printer drivers have been causing spooler failures.

Print administrator delegation
On computers running Windows Server 2008 R2, the default permissions do not allow non-administrative users to perform any administrative print operations.

However, an administrator can delegate specific administrative printer tasks to non-administrative users, which reduces costs. Security risks are not introduced because non-administrative personnel are not granted system administrative rights.

Print Management snap-in improvements
Improvements to the Print Management snap-in enable you to better manage print servers, print queues, and print drivers. In Windows Server 2008 R2, the Print Management snap-in includes better support for driver management and the ability to view all print drivers installed on the network. You can now examine driver versions, driver package information, and manage driver isolation.

CSR performance improvements
In Windows Server 2008 R2, the frequency of CSR caching has been increased. Subsequently, the number of printer spooler requests that are made by applications has been reduced, which improves overall printing system performance and reduces network load.

XPS print path improvements
XPS enables Windows applications to produce rich content that can be preserved through the entire print system without costly conversions or data loss. XPS can replace a document presentation language (such as Rich Text Format (RTF)), a print spooler format (such as Windows Metafile Format (WMF)), and a page description language (such as PostScript).

In Windows Server 2008, an XPS-based print path was introduced to enhance the fidelity and performance of Windows printing. In Windows Server 2008 R2, the use of XPS in the printing system is extended and improved upon in several areas: "what you see is what you get" (WYSIWYG) printing, improved print fidelity and color support, XPS Viewer enhancements, new rendering and rasterizing services for printer drivers, and significantly improved print performance. In addition, this functionality is now available in an unmanaged application programming interface (API) layer for application developers.

Location-aware printing
In Windows Server 2008 R2, the Default Printer setting is now location aware. A mobile or laptop user can set a different default printer for each network that they connect to. They may have a default printer set for home, and a different default printer set for office use. Their laptop can now automatically select the correct default printer, depending on where the user is currently located.

Distributed Scan Server role service
As more scanners become network enabled, administrators need a way to manage these devices on their network without having to use the applications from different hardware vendors. Additionally, scanners need to be part of an organization's document workflow process.

In Windows Server 2008 R2, Distributed Scan Server is a new role service in the Print and Document Services role. You can use Distributed Scan Server to monitor Web Services on Devices (WSD)–enabled network scanners and create and manage scan processes. Distributed Scan Server makes it possible to easily use scanners to integrate paper-based information into corporate computer-based networks more effectively.

A scan process is a rule or set of instructions that defines how a document is scanned, where or who it is delivered to, and what users and groups are allowed to apply the rule to their scanned documents. A user selects a scan process at the front panel of a scanner that supports WSD at the time the document is scanned.

Scan settings include image resolution settings, color format settings, and file types. These settings are defined as part of the scan process rules. These settings can also be validated to make sure the settings are compatible with the scanner associated with the particular scan process. You can configure the scan process so that a user can override the scan settings at the scanner. Scanned document images can be sent to a network shared folder, a Windows SharePoint Web site, e-mail recipients, or any combination of these.

Chapter 16 – What's New in Remote Desktop Services

What's New in Remote Desktop Services

Remote Desktop Services, formerly Terminal Services, provides technologies that enable users to access session-based desktops, virtual machine-based desktops, or applications in the datacenter from both within a corporate network and from the Internet. Remote Desktop Services enables a rich-fidelity desktop or application experience, and helps to securely connect remote users from managed or unmanaged devices.

In Windows Server 2008 R2 with Service Pack 1 (SP1), Microsoft RemoteFX has been added to Remote Desktop Services. RemoteFX enables a rich PC experience for virtual machine users, through a 3D adapter and USB redirection. The 3D scenarios in virtual desktops provide a virtualized graphics processing unit (GPU) within the virtual machine. RemoteFX also provides intelligent capture and compression that adapts for the best user experience and scale both for virtual and session-based desktops.

In Windows Server 2008 R2, all Remote Desktop Services role services have been renamed. The following table lists both the former name and the new name of each Remote Desktop Services role service.

Previous name	Name in Windows Server 2008 R2
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)

In addition to the Remote Desktop Services role services names, the name of the Remote Desktop Services management tools have also changed.

Previous name	Name in Windows Server 2008 R2
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

The following topics describe changes in Remote Desktop Services functionality available in this release:

- Remote Desktop Session Host
- Remote Desktop Virtualization Host
- Remote Desktop Connection Broker
- Remote Desktop Web Access
- Remote Desktop Gateway
- RemoteApp and Desktop Connection
- Remote Desktop Licensing
- Remote Desktop Client Experience
- Remote Desktop Services Management
- Microsoft RemoteFX

Remote Desktop Session Host

What are the major changes?

The Remote Desktop Session Host (RD Session Host) role service, formerly the Terminal Server role service, has been enhanced in Windows Server 2008 R2. The following changes are available in Windows Server 2008 R2:

- Client experience configuration page
- Per-user RemoteApp filtering
- Fair Share CPU Scheduling
- Windows Installer RDS Compatibility

- Roaming user profile cache management
- Remote Desktop IP Virtualization

Who will be interested in these features?

The improvements to the RD Session Host role service will be of interest to organizations that currently use or are interested in Remote Desktop Services.

You may also be interested in these improvements in the RD Session Host role service if you want to support any of the following scenarios:

- Your organization has programs running on an RD Session Host server that require IP addresses to be assigned on either a per session or per program basis.
- Remote desktop users within your organization routinely install programs within their RD Session Host session.

What new functionality do these features provide?

The new functionality provided by these new features in the RD Session Host role service is described in the following sections.

Client experience configuration page
The client experience configuration page is available when installing the RD Session Host role service by using Server Manager. The client experience configuration page allows you to configure the following functionality:

- **Audio and video playback redirection.** Audio and video playback redirection allows users to redirect the audio and video output of a local computer to an RD Session Host session.
- **Audio recording redirection.** Audio recording redirection allows users to redirect the output of an audio recording device, such as a microphone, from the local computer to an RD Session Host session.
- **Desktop composition.** Desktop composition provides users with the user interface elements of the Windows® Aero® desktop experience within their RD Session Host session.

Note

Configuring any of these features also installs the Desktop Experience role service and starts the Windows Audio service on the RD Session Host server.

Why are these changes important?
This page centralizes the client experience configuration into Server Manager.

Are there any dependencies?
To take advantage of the new client experience features, the client must be running Remote Desktop Connection (RDC) 7.0.

Per-user RemoteApp filtering
In Remote Desktop Services in Windows Server 2008 R2, you can filter the list of RemoteApp programs that are available to a user account when logged on to RD Web Access.

Why is this change important?
Prior to Windows Server 2008 R2, all RemoteApp programs were shown to every user that logged on to RD Web Access, regardless of whether they had access to run the program.

Fair Share CPU Scheduling
Fair Share CPU Scheduling is a new feature included with Remote Desktop Services in Windows Server 2008 R2. Fair Share CPU Scheduling dynamically distributes processor time across sessions based on the number of active sessions and load on those sessions by using the kernel-level scheduling mechanism included with Windows Server 2008 R2. On an RD Session Host server, one user will not affect the performance of another user's session, even if the RD Session Host server is under a high load.

Fair Share CPU Scheduling is enabled by default. You can disable this feature by configuring the following registry entry to 0:
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\SessionManager\DFSS\EnableDFSS.

Why is this change important?
Prior to Windows Server 2008 R2, the Windows scheduler provided a fair scheduling policy by distributing the processor time evenly across all threads at a given priority level. Priority could be adjusted by using management software to give one thread preference over another. In an environment with multiple users, this scheduling policy provided a good way to throttle any one user from completely monopolizing the CPU, but was unable to evenly distribute the processor time in the presence of dynamic loads.

Windows Installer RDS Compatibility
Windows Installer RDS Compatibility is a new feature included with Remote Desktop Services in Windows Server 2008 R2. With Remote Desktop Services in Windows Server 2008 R2, per user application installations are queued by the RD Session Host server and then handled by the Windows Installer.

In Windows Server 2008 R2 you can install a program on the RD Session Host server just like you would install the program on a local desktop. Ensure, however, that you install the program for all users and that all components of the program are installed locally on the RD Session Host server .

Windows Installer RDS Compatibility is enabled by default. You can disable this feature by configuring the following registry entry to 0: **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Terminal Services\TSAppSrv\TSMSI\Enable**.

Why is this change important?
Prior to Remote Desktop Services in Windows Server 2008 R2, only one Windows Installer installation was supported at a time. For applications that required per user configurations, such as Microsoft Office Word, an administrator needed to pre-install the application, and application developers would need to test these applications on both the remote desktop client and the RD Session Host server. Windows Installer RDS Compatibility queues the installation requests and processes them one at a time.

Roaming user profile cache management
A new Group Policy setting is available for Remote Desktop Services in Windows Server 2008 R2 that limits the size of the overall profile cache. If the size of the profile cache exceeds the configured size, Remote Desktop Services deletes the least recently used profiles until the overall cache goes below the quota.

You can configure the maximum size of the roaming user profile cache on an RD Session Host server by applying the **Limit the size of the entire roaming user profile cache** Group Policy setting. The Group Policy setting is located in **Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Profiles**. If you enable this policy setting, you must specify a monitoring interval (in minutes) and a maximum size (in gigabytes) for the entire roaming user profile cache. The monitoring interval determines how often the size of the roaming user profile cache is checked.

Note

If you are using the Local Group Policy Editor, "Policies" is not part of the node path.

Why is this change important?
A Remote Desktop Services environment can potentially have hundreds of distinct users. Whereas caching of roaming user profiles is enabled for better end-user experience, this profile cache can grow very large and may potentially overrun the available disk space on the server.

Remote Desktop IP Virtualization
Remote Desktop IP Virtualization allows IP addresses to be assigned to remote desktop connections on a per session or per program basis. Remote Desktop IP Virtualization is configured on the **RD IP Virtualization** tab of the Remote Desktop Session Host Configuration tool.

If you assign IP addresses for multiple programs, they will share a session IP address. If you have more than one network adapter on the computer, you must also choose one network adapter for Remote Desktop IP Virtualization.

Why is this change important?
Some programs require that each instance of the application be assigned a unique IP address. Prior to Windows Server 2008 R2, all sessions on an RD Session Host server shared the IP address assigned to the RD Session Host server. With Windows Server 2008 R2, you specify a network ID that Remote Desktop IP Virtualization uses to assign IP addresses on a per session or per program basis.

Which editions include these features?

RD Session Host is available in the following editions of Windows Server 2008 R2:

- Windows Server 2008 R2 Standard
- Windows Server 2008 R2 Enterprise
- Windows Server 2008 R2 Datacenter

RD Session Host is not available in the following editions of Windows Server 2008 R2:

- Windows Web Server 2008 R2
- Windows Server 2008 R2 for Itanium-Based Systems

Remote Desktop Licensing

What are the major changes?

Remote Desktop Licensing (RD Licensing), formerly Terminal Services Licensing (TS Licensing), is a role service in the Remote Desktop Services server role included with Windows Server 2008 R2. RD Licensing manages the Remote Desktop Services client access licenses (RDS CALs) that are required for each device or user to connect to a Remote Desktop Session Host (RD Session Host) server. You use Remote Desktop Licensing Manager (RD Licensing Manager) to install, issue, and track the availability of RDS CALs on a Remote Desktop license server.

The following changes are available in Windows Server 2008 R2:

- Automatic license server discovery no longer supported for RD Session Host servers
- Changes to Licensing tab in Remote Desktop Session Host Configuration
- The Manage RDS CALs Wizard
- Service Connection Point registration
- Single RDS CAL pack support

Who will be interested in these features?

The improvements to the RD Licensing role service will be of interest to organizations that currently use or are interested in deploying Remote Desktop Services in their environment.

What new functionality do these features provide?

The new functionality provided by these features in the RD Licensing role service is described in the following sections.

Automatic license server discovery no longer supported for RD Session Host servers
In Windows Server 2008 R2, you must specify the name of a license server for the RD Session Host server to use by using Remote Desktop Session Host Configuration.

However, for Windows Server 2008, Windows Server 2003, or Windows 2000 Server, you must specify a discovery scope when you install the RD Licensing role service, which determines how the Remote Desktop license server is automatically discoverable by terminal servers that are running these earlier operating systems.

Why is this change important?
Prior to Windows Server 2008 R2, the license server was automatically discovered on the network. This discovery is no longer supported for an RD Session Host server that is running Windows Server 2008 R2.

Changes to Licensing tab in Remote Desktop Session Host Configuration
In Remote Desktop Session Host Configuration in Windows Server 2008 R2, you must specify a license server for the RD Session Host server to use. You can either choose from a list of known license servers or manually enter the name. License servers that are registered as a service connection point in Active Directory® Domain Services (AD DS) will appear in the list of known license servers in Remote Desktop Session Host Configuration. You can add more than one license server for the RD Session Host server to use. If more than one license server is added, the RD Session Host server contacts the license servers in the order in which they appear in the **Specified license servers** box on the **Licensing** tab in Remote Desktop Session Host Configuration.

The Manage RDS CALs Wizard
In Windows Server 2008 R2, a new wizard is available in Remote Desktop Licensing Manager (RD Licensing Manager) that allows you to do the following:

- Migrate RDS CALs from one license server to another license server.
- Rebuild the RD Licensing database.

Note

You can only use the Manage RDS CALs Wizard for a license server that is running Windows Server 2008 R2.

You might want to migrate RDS CALs from one license server to another license server if you are replacing one license server with the other one or if one license server is no longer functioning. By using the Manage RDS CALs Wizard, you can automatically migrate RDS CALs from one license server to another license server. However, if you are migrating RDS CALs from a license server that is not running Windows Server 2008 R2, you must manually remove the RDS CALs from the original license server after you have finished the migration process.

Caution

Rebuilding the RD Licensing database will delete any RDS CALs that are currently installed on the license server. You must reinstall those RDS CALs onto the license server after the database is rebuilt.

Service Connection Point registration
Registration of the license server in AD DS enables a list of valid and published license servers to be listed during manual licensing configuration for an RD Session Host server. When the RD Licensing role service in Windows Server 2008 R2 is added by using Server Manager, the license server attempts to register as a service connection point (SCP) in AD DS. When a license server is registered as an SCP, it will appear in the list of known license servers in Remote Desktop Session Host Configuration. If AD DS is not available during installation of the RD Licensing role service, you can manually register the license server by using Review Configuration in Remote Desktop Licensing Manager.

Single RDS CAL pack support
Prior to Windows Server 2008 R2, RDS CALs were sold in packs of 5 and 20. In Windows Server 2008 R2, single RDS CALs can be purchased and installed.

Which editions include these features?

RD Licensing is available in the following editions of Windows Server 2008 R2:

- Windows Server 2008 R2 Standard
- Windows Server 2008 R2 Enterprise
- Windows Server 2008 R2 Datacenter

RD Licensing is not available in the following editions of Windows Server 2008 R2:

- Windows Web Server 2008 R2
- Windows Server 2008 R2 for Itanium-Based Systems

Remote Desktop Connection Broker

What are the major changes?

Remote Desktop Connection Broker (RD Connection Broker), formerly Terminal Services Session Broker (TS Session Broker), is used to provide users with access to RemoteApp and Desktop Connection. RemoteApp and Desktop Connection provides users a single, personalized, and aggregated view of RemoteApp programs, session-based desktops, and virtual desktops to users. RD Connection Broker supports load balancing and reconnection to existing sessions on virtual desktops, Remote Desktop sessions, and RemoteApp programs accessed by using RemoteApp and Desktop Connection. RD Connection Broker also aggregates RemoteApp sources from multiple Remote Desktop Session Host (RD Session Host) servers that may host different RemoteApp programs.

To configure which RemoteApp programs and virtual desktops are available through RemoteApp and Desktop Connection, you must add the RD Connection Broker role service on a computer running Windows Server 2008 R2, and then use Remote Desktop Connection Manager (RD Connection Manager).

For more information, see RemoteApp and Desktop Connection.

Who will be interested in this feature?

The improvements to the RD Connection Broker role service will be of interest to organizations that are implementing either a Virtual Desktop Infrastructure (VDI) or are deploying session-based desktops or RemoteApp programs. Additionally, these improvements will be of interest to organizations that currently use or are interested in Remote Desktop Services.

What does RD Connection Broker do?

RD Connection Broker extends the TS Session Broker capabilities included in Windows Server 2008 by creating a unified administrative experience for traditional session-based remote desktops and virtual machine-based remote desktops. A virtual machine-based remote desktop can be either a personal virtual desktop or part of a virtual desktop pool. In the case of a personal virtual desktop, there is a one-to-one mapping of virtual machines to users. Each user is assigned a personal virtual desktop that can be personalized and customized. These changes are available to users each time that they log on to their personal virtual desktop. For a virtual desktop pool, a single image is replicated across many virtual machines. As users connect to the shared virtual desktop pool, they are dynamically assigned a virtual desktop. Because users may not be assigned the same virtual desktop when they connect, any personalization and customization made by a user are not saved. If you choose to use a virtual desktop pool and users need their personalization and customizations saved, you can use roaming profiles and folder redirection.

Which editions include this feature?

RD Connection Broker is available in the following editions of Windows Server 2008 R2:

- Windows Server 2008 R2 Standard
- Windows Server 2008 R2 Enterprise
- Windows Server 2008 R2 Datacenter

RD Connection Broker is not available in the following editions of Windows Server 2008 R2:

- Windows Web Server 2008 R2
- Windows Server 2008 R2 for Itanium-Based Systems

Remote Desktop Gateway

What are the major changes?

Remote Desktop Gateway (RD Gateway), formerly Terminal Services Gateway (TS Gateway), is a role service in the Remote Desktop Services server role included with Windows Server® 2008 R2 that enables authorized remote users to connect to resources on an internal corporate or private network, from any Internet-connected device that can run the Remote Desktop Connection (RDC) client. The network resources can be Remote Desktop Session Host (RD Session Host) servers, RD Session Host servers running RemoteApp programs, or computers and virtual desktops with Remote Desktop enabled. RD Gateway uses the Remote Desktop Protocol (RDP) over HTTPS to establish a secure, encrypted connection between remote users on the Internet and internal network resources.

The following changes are available in Windows Server 2008 R2:

- Configurable idle and session timeouts
- Background session authentication and authorization
- System and logon messages
- Device redirection enforcement
- Network Access Protection (NAP) remediation
- Pluggable authentication and authorization

Who will be interested in these features?

The improvements to the RD Gateway role service will be of interest to organizations that currently use or are interested in extending Remote Desktop Services to clients that are not directly connected to the corporate network.

Are there any special considerations?

To take advantage of the new functionality introduced for RD Gateway in Windows Server 2008 R2, you must use the following:

- A Windows Server 2008 R2 server configured as an RD Session Host server.
- A Windows Server 2008 R2 server configured as an RD Gateway server.
- Remote Desktop clients using Remote Desktop Connection (RDC) 7.0.

Note

Existing functionality will still work with terminal servers running Windows Server 2008 or Windows Server 2003.

What new functionality do these features provide?

The new functionality provided by these features in the RD Gateway role service is described in the following sections.

Configurable idle and session timeouts
RD Gateway allows you to configure idle and session timeouts on the RD Gateway server. An idle timeout provides the ability to reclaim resources used by inactive user sessions without affecting the user's session or data. This helps free up resources on the RD Gateway server. After being disconnected, the user will be able to reestablish the session by using RDC. A session timeout provides the capability to periodically enforce new policies on active user connections. This ensures that any system changes to user properties, such as domain accounts, Remote Desktop connection authorization policy (RD CAP) changes, or Remote Desktop resource authorization policy (RD RAP) changes, are enforced on existing sessions.

- An idle timeout provides the ability to reclaim resources used by inactive user sessions without affecting the user's session or data. This helps free up resources on the RD Gateway server. After being disconnected, the user will be able to reestablish the session by using RDC.

- A session timeout provides the capability to periodically enforce new policies on active user connections. This ensures that any system changes to user properties, such as domain accounts, RD CAP changes, or RD RAP changes, are enforced on existing sessions.

The idle and session timeouts are configured on the **Timeout** tab of the RD CAP by using Remote Desktop Gateway Manager.

Why is this change important?
Configurable idle and session timeouts with RD Gateway help you gain better control of users who are connecting through RD Gateway. Timeouts allow you to reclaim resources from sessions that are not currently in use, helping to ensure that idle sessions are not wasting system resources. User properties that are changed can still be enforced for users accessing the system by using remote desktop sessions.

Background session authentication and authorization
When a timeout has been reached, the remote session can be disconnected or the session can be silently re-authenticated and reauthorized. If the option to silently re-authenticate and reauthorize is selected, after a configured session timeout has been reached, sessions for users whose property information has not changed are not affected, and authentication and authorization requests are sent in the background.

Why is this change important?
Background authentication and authorization requests are done automatically and require no user interaction.

System and logon messages
System and logon messages can be added to RD Gateway in Windows Server 2008 R2 and displayed to the remote desktop user. System messages can be used to inform users of server maintenance issues such as shutdown and restarts. Logon messages can be used to display a logon notice to users before they gain access to remote resources.

You can configure RD Gateway to only allow connections from remote desktop clients that support system and logon messages. Remote desktop clients must be running RDC 7.0 to connect by using this setting.

The system and logon messages are configured on the **Messaging** tab of the RD Gateway server Properties, by using Remote Desktop Gateway Manager.

Why is this change important?
Messaging can be used to keep remote desktop clients more informed. System messages can be used to inform users of upcoming server downtimes. Logon messages can be used to display legal information that the remote desktop user must acknowledge before starting an RD Gateway session.

Device redirection enforcement
An RD Gateway server running Windows Server 2008 R2 includes the option to allow remote desktop clients to only connect to RD Session Host servers that enforce device redirection. RDC 7.0 is required for device redirection to be enforced by the RD Session Host server running Windows Server 2008 R2.

Device redirection enforcement is configured on the **Device Redirection** tab of the RD CAP by using Remote Desktop Gateway Manager.

Why is this change important?
Device redirection enforcement helps prevent malicious code on remote clients from overriding security polices set by an administrator.

Network Access Protection (NAP) remediation
An RD Gateway server running Windows Server 2008 R2 enables you to update client computers that are not in compliance with the health policy. This helps keep managed clients in compliance with the latest software updates. Administrators can set CAP policies so that unmanaged clients do not receive updates, and are only provided health feedback allowing users to manually update their systems.

Why is this change important?
NAP remediation allows you to manage remote clients by updating them with the latest software updates and settings. This helps keep remote clients in compliance with network security policies.

Pluggable authentication and authorization
Pluggable authentication provides APIs which can be used to write authentication and authorization plug-ins for integration with RD Gateway. RD Gateway exposes interfaces for authoring custom authentication and authorization plug-ins.

Why is this change important?
Pluggable authentication and authorization allows you to use non-Windows-based methods for authentication and authorization. You can use this to develop your own custom plug-ins to better fit your network admission requirements.

Remote Desktop Web Access

What are the major changes?

Remote Desktop Web Access (RD Web Access), formerly Terminal Services Web Access (TS Web Access), enables users to access RemoteApp and Desktop Connection through a Web browser. The RD Web Access role service has been enhanced in Windows Server 2008 R2. The following improvements to RD Web Access are available in Windows Server 2008 R2:

- Forms-based authentication
- Per user RemoteApp program filtering
- Single sign-on between Remote Desktop Session Host (RD Session Host) and RD Web Access
- Public and private computer option

Who will be interested in these features?

The improvements to the RD Web Access role service will be of interest to organizations that currently use or are interested in Remote Desktop Services.

What new functionality do these features provide?

The new functionality provided by these features in the RD Web Access role service is described in the following sections.

Forms-based authentication
Forms-based authentication is an ASP.NET authentication service that enables applications to provide their own logon page and do their own credential verification. ASP.NET authenticates users, redirects unauthenticated users to the logon page, and performs all the necessary cookie management.

Why is this change important?
Forms-based authentication with RD Web Access provides a user in your organization a better logon experience. Additionally, it allows the administrator to customize the RD Web Access logon page to display company branding or other important information.

Per user RemoteApp program filtering
RD Web Access can filter the view on a per user account basis so that the user logging on to RD Web Access only sees the programs that the administrator configured for them to see.

Why is this change important?
Prior to Windows Server 2008 R2, all RemoteApp programs were shown to every user that logged on to RD Web Access.

Single sign-on between RD Session Host and RD Web Access
Single sign-on allows customers the ability to enter their user name and password only once when connecting to a RemoteApp program by using RD Web Access.

Why is this change important?
Prior to Windows Server 2008 R2, when a user connected to a RemoteApp program by using RD Web Access, the user was prompted for credentials twice. One set of credentials was used to authenticate the user to the RD Web Access server and the other set was used to authenticate the user to the RD Session Host server hosting the RemoteApp program. Asking for the same user credentials twice led to a bad user experience. In Windows Server 2008 R2, you are only prompted once.

Important

Single sign-on requires that your RDP files are digitally signed by a trusted publisher. The certificate used to sign the RemoteApp programs must be present in the Trusted Root Certification Authorities store on the client computer.

Are there any dependencies?
To take advantage of the new single sign-on features, the client must be running Remote Desktop Connection (RDC) 7.0.

Public and private computer option
The RD Web Access Web page can be accessed via public or private mode. When you select public mode, your user name is not remembered in the Web browser and RD Web Access cookies storing the user name time out in 20 minutes. When you select private mode, cookies storing the user name are available for four hours. In either public or private mode, passwords are not stored.

Why is this change important?
Public mode is recommended when you are using a computer that is located in a public place. Private mode is recommended for computers that you use often, such as a home or office computer.

Remote Desktop Virtualization Host

What are the major changes?

Remote Desktop Virtualization Host (RD Virtualization Host) is a new Remote Desktop Services role service included with Windows Server 2008 R2. RD Virtualization Host integrates with the Hyper-V™ role to provide virtual machines that can be used as personal virtual desktops or virtual desktop pools by using RemoteApp and Desktop Connection. User accounts can be assigned a unique personal virtual desktop or be redirected to a virtual desktop pool where a virtual desktop is dynamically assigned. RD Virtualization Host is an important component to the Virtual Desktop Infrastructure (VDI) solution offered by Microsoft.

What does Remote Desktop Virtualization Host do?

An administrator can make personal virtual desktops or virtual desktop pools available to users by using either RemoteApp and Desktop Connection or Remote Desktop Web Access (RD Web Access). These virtual desktops are virtual machines hosted on a computer that is running Windows Server 2008 R2 on which Hyper-V and RD Virtualization Host are also installed.

With a personal virtual desktop, a user is assigned a personal virtual desktop in Active Directory Domain Services (AD DS). A personal virtual desktop can be assigned to only one user account. All customizations that the user does to their personal virtual desktop are saved and available to them when they log on to the personal virtual desktop again.

A virtual desktop pool requires that virtual machines are identically configured and should not already be assigned to a user as a personal virtual desktop. Because the virtual machines are identically configured, the user will see the same virtual desktop, regardless of which virtual machine in the virtual desktop pool the user connects to by using RemoteApp and Desktop Connection. Also, you can configure virtual desktop pools to roll back to a previous state when a user account logs off from the computer.

RemoteApp and Desktop Connection

What are the major changes?

In Windows Server 2008, Terminal Services introduced RemoteApp programs, which are programs that are accessed remotely through Remote Desktop Services and appear as if they are running on the end user's local computer. In Windows Server 2008 R2, Remote Desktop Services provides administrators the ability to group and personalize RemoteApp programs as well as virtual desktops and make them available to end users on the **Start** menu of a computer that is running Windows® 7. This new feature is called RemoteApp and Desktop Connection.

RemoteApp and Desktop Connection provides a personalized view of RemoteApp programs, session-based desktops, and virtual desktops to users. When a user starts a RemoteApp program or a session-based desktop, a Remote Desktop Services session is started on the Remote Desktop Session Host (RD Session Host) server that hosts the remote desktop or RemoteApp program. If a user connects to a virtual desktop, a remote desktop connection is made to a virtual machine that is running on a Remote Desktop Virtualization Host (RD Virtualization Host) server. To configure which RemoteApp programs, session-based desktops, and virtual desktops are available through RemoteApp and Desktop Connection, you must add the Remote Desktop Connection Broker (RD Connection Broker) role service on a computer that is running Windows Server 2008 R2, and then use Remote Desktop Connection Manager.

In Windows 7 and Windows Server 2008 R2, you configure RemoteApp and Desktop Connection by using Control Panel. After RemoteApp and Desktop Connection is configured, RemoteApp programs, session-based desktops, and virtual desktops that are part of this connection are available to users on the **Start** menu of their computer. Any changes that are made to RemoteApp and Desktop Connection, such as adding or removing RemoteApp programs or virtual desktops, are automatically updated on the client and on the **Start** menu.

Users can use the new RemoteApp and Desktop Connection notification area icon to:

- Identify when they are connected to RemoteApp and Desktop Connection.
- Disconnect from RemoteApp and Desktop Connection if the connection is no longer needed.

Administrators can create a client configuration file (.wcx) and distribute it to users within their organization so that the user can automatically configure RemoteApp and Desktop Connection. Administrators can also write and distribute a script to run the client configuration file silently so that RemoteApp and Desktop Connection is set up automatically when the user logs on to their account on a Windows 7 computer.

Who will be interested in this feature?

RemoteApp and Desktop Connection will be of interest to organizations that are interested in assigning programs or virtual desktops to users and providing a seamless user experience that is tightly integrated into the Windows 7 client experience.

Are there any special considerations?

You must have Remote Desktop Web Access (RD Web Access) deployed within your organization to provide RemoteApp and Desktop Connection to the **Start** menu on a Windows 7 computer.

Remote Desktop Client Experience

What are the major changes?

The Remote Desktop Connection client experience has been enhanced for computers running Windows 7 that are connecting to a Remote Desktop Session Host (RD Session Host) server running Windows Server 2008 R2.

The following changes are available in Windows Server 2008 R2:

- **Audio and video playback.** In Windows Server 2008 R2, audio and video content, played back by using Windows Media Player, is redirected from the RD Session Host server to the client computer in its original format and rendered by using the client computer's resources. Other multimedia content such as Silverlight and Windows Presentation Foundation are rendered on the server. The bitmaps are then compressed and sent over to the client.

- **Multiple monitor support.** Remote Desktop Connection (RDC) 7.0 and Windows Server 2008 R2 enable support for up to 16 monitors. This feature supports connecting to a remote session with any monitor configuration that is supported on the client computer. Programs function just like they do when they are running on the client computer.

  Caution

  Desktop composition is not supported on an RD Session Host session with multiple monitors.

- **Audio recording redirection.** RDC 7.0 and Windows Server 2008 R2 redirect audio recording devices, such as microphones, from the client computer to the remote desktop session. This may be useful for organizations that use voice chat or Windows Speech Recognition.

- **Desktop composition.** RDC 7.0, Windows 7, and Windows Server 2008 R2 support Windows Aero within an RD Session Host session.

  Caution

  Desktop composition is not supported in a remote session from Windows Vista® to Windows 7, or in a remote session from Windows 7 to Windows Vista even if the RDC 7.0 client is installed. You must be using Windows 7 or Windows Server 2008 R2 to take advantage of the desktop composition feature.

- **Language bar redirection.** In RDC 7.0 and Windows Server 2008 R2, you can use the language bar on the client computer to control the language settings within your RemoteApp programs.

These new capabilities, enabled with Windows Server 2008 R2 in combination with Windows 7, significantly improve the experience of remote users, making it more similar to the experience of users accessing local computing resources.

Who will be interested in this feature?

The improvements to the Remote Desktop Connection client experience will be of interest to organizations that currently use or are interested in Remote Desktop Services.

Chapter 17 – What's New in Security in Windows Server 2008 R2

What are the major changes?

The following topics are available in Changes in Functionality from Windows Server 2008 to Windows Server 2008 R2:

- What's New in AppLocker
- What's New in Biometrics
- What's New in Service Accounts
- What's New in Smart Cards
- What's New in User Account Control
- What's New in Windows Security Auditing

What's New in AppLocker

What are the major changes?

AppLocker™ is a new feature in Windows® 7 and Windows Server® 2008 R2 that replaces the Software Restriction Policies feature. AppLocker contains new capabilities and extensions that reduce administrative overhead and help administrators control how users can access and use files, such as .exe files, scripts, Windows Installer files (.msi and .msp files), and DLLs.

What does AppLocker do?

Using AppLocker, you can:

- Define rules based on file attributes derived from the digital signature, including the publisher, product name, file name, and file version. For example, you can create rules based on the publisher and file version attributes that are persistent through updates, or you can create rules that target a specific version of a file.

Important
AppLocker rules specify which files are allowed to run. Files that are not included in rules are not allowed to run.

- Assign a rule to a security group or an individual user.

> **Note**
>
> You cannot assign AppLocker rules to Internet zones, individual computers, or registry paths.

- Create exceptions for .exe files. For example, you can create a rule that allows all Windows processes to run except Regedit.exe.
- Use audit-only mode to identify files that would not be allowed to run if the policy were in effect.
- Import and export rules.

Who will be interested in this feature?

AppLocker can help organizations that want to:

- Limit the number and type of files that are allowed to run by preventing unlicensed or malicious software from running and by restricting the ActiveX controls that are installed.
- Reduce the total cost of ownership by ensuring that workstations are homogeneous across their enterprise and that users are running only the software and applications that are approved by the enterprise.
- Reduce the possibility of information leaks from unauthorized software.

AppLocker may also be of interest to organizations that currently use Group Policy objects (GPOs) to manage Windows-based computers or have per-user application installations.

Are there any special considerations?

- By default, AppLocker rules do not allow users to open or run any files that are not specifically allowed. Administrators should maintain an up-to-date list of allowed applications.
- Expect an increase in the number of help desk calls initially because of blocked applications. As users begin to understand that they cannot run applications that are not allowed, the help desk calls may decrease.
- There is minimal performance degradation because of the runtime checks.
- Because AppLocker is similar to the Group Policy mechanism, administrators should understand Group Policy creation and deployment.
- AppLocker rules cannot be used to manage computers running a Windows operating system earlier than Windows 7.
- If AppLocker rules are defined in a GPO, only those rules are applied. To ensure interoperability between Software Restriction Policies rules and AppLocker rules, define Software Restriction Policies rules and AppLocker rules in different GPOs.

- When an AppLocker rule is set to **Audit only**, the rule is not enforced. When a user runs an application that is included in the rule, the application is opened and runs normally, and information about that application is added to the AppLocker event log.

What's New in Biometrics

What's new in biometrics?

A growing number of computers, particularly portable computers, include embedded fingerprint readers. Fingerprint readers can be used for identification and authentication of users in Windows. Until now, there has been no standard support for biometric devices or for biometric-enabled applications in Windows. Computer manufacturers had to provide software to support biometric devices in their products. This made it more difficult for users to use the devices and administrators to manage the use of biometric devices.

Windows 7 includes the Windows Biometric Framework that exposes fingerprint readers and other biometric devices to higher-level applications in a uniform way, and offers a consistent user experience for discovering and launching fingerprint applications. It does this by providing the following:

- A **Biometric Devices** Control Panel item that allows users to control the availability of biometric devices and whether they can be used to log on to a local computer or domain.
- Device Manager support for managing drivers for biometric devices.
- Credential provider support to enable and configure the use of biometric data to log on to a local computer and perform UAC elevation.
- Group Policy settings to enable, disable, or limit the use of biometric data for a local computer or domain. Group Policy settings can also prevent installation of biometric device driver software or force the biometric device driver software to be uninstalled.
- Biometric device driver software available from Windows Update.

Who will want to use biometric devices?

Fingerprint biometric devices offer a convenient way for users to log on to computers and grant elevation through UAC.

What are the benefits of the new biometric features?

The new biometric features provide a consistent way to implement fingerprint biometric–enabled applications and manage fingerprint biometric devices on stand-alone computers or on a network. The Windows Biometric Framework makes biometric devices easier for users and for administrators to configure and control on a local computer or in a domain.

What's the impact of these changes on biometrics?

The introduction of the Windows Biometric Framework allows the integration of fingerprint biometric devices in Windows. It offers a consistent user experience for logging on to Windows and performing UAC elevation. In addition, it provides a common set of discovery and integration points that offers a more consistent user experience across devices and applications. The Windows Biometric Framework also includes management functions that allow administrators to control the deployment of biometric fingerprint devices in the enterprise.

What's New in Service Accounts

What's new in service accounts?

Two new types of service accounts are available in Windows Server® 2008 R2 and Windows® 7—the managed service account and the virtual account. The managed service account is designed to provide crucial applications such as SQL Server and IIS with the isolation of their own domain accounts, while eliminating the need for an administrator to manually administer the service principal name (SPN) and credentials for these accounts. Virtual accounts in Windows Server 2008 R2 and Windows 7 are "managed local accounts" that can use a computer's credentials to access network resources.

Who will want to use service accounts?

Administrators will want to use managed service accounts to enhance security while simplifying or eliminating password and SPN management.

Virtual accounts simplify service administration by eliminating password management and allowing services to access the network with the computer's account credentials in a domain environment.

What are the benefits of new service accounts?

In addition to the enhanced security that is provided by having individual accounts for critical services, there are four important administrative benefits associated with managed service accounts:

- Managed service accounts allow administrators to create a class of domain accounts that can be used to manage and maintain services on local computers.
- Unlike with regular domain accounts in which administrators must reset passwords manually, the network passwords for these accounts will be reset automatically.
- Unlike with normal local computer and user accounts, the administrator does not have to complete complex SPN management tasks to use managed service accounts.
- Administrative tasks for managed service accounts can be delegated to non-administrators.

What's the impact of these changes on account management?

Managed service accounts can reduce the amount of account management needed for critical services and applications.

Are there any special considerations for using the new service account options?

To use managed service accounts and virtual accounts, the client computer on which the application or service is installed must be running Windows Server 2008 R2 or Windows 7. In Windows Server 2008 R2 and Windows 7, one managed service account can be used for services on a single computer. Managed service accounts cannot be shared between multiple computers and cannot be used in server clusters where a service is replicated on multiple cluster nodes.

Windows Server 2008 R2 domains provide native support for both automatic password management and SPN management. If the domain is running in Windows Server 2003 mode or Windows Server 2008 mode, additional configuration steps will be needed to support managed service accounts. This means that:

- If the domain controller is running Windows Server 2008 R2 and the schema has been upgraded to support managed service accounts, both automatic password and SPN management are available.

- If the domain controller is on a computer running Windows Server 2008 or Windows Server 2003 and the Active Directory schema has been upgraded to support this feature, managed service accounts can be used and service account passwords will be managed automatically. However, the domain administrator using these server operating systems will still need to manually configure SPN data for managed service accounts.

To use managed service accounts in Windows Server 2008, Windows Server 2003, or mixed-mode domain environments, the following schema changes must be applied:

- Run **adprep /forestprep** at the forest level.
- Run **adprep /domainprep** in every domain where you want to create and use managed service accounts.
- Deploy a domain controller running Windows Server 2008 R2 in the domain to manage managed service accounts by using Windows PowerShell cmdlets.

What's New in Smart Cards

What's new in smart cards?

Windows 7 features enhanced support for smart card–related Plug and Play and the Personal Identity Verification (PIV) standard from the National Institute of Standards and Technology (NIST).

This means that users of Windows 7 can use smart cards from vendors who have published their drivers through Windows Update without needing special middleware. These drivers are downloaded in the same way as drivers for other devices in Windows.

When a PIV-compliant smart card is inserted into a smart card reader, Windows attempts to download the driver from Windows Update. If an appropriate driver is not available from Windows Update, a PIV-compliant minidriver that is included with Windows 7 is used for the card.

Who will want to use smart cards?

Network administrators who want to enhance the security of the organization's computers, particularly portable computers used by remote users, will appreciate the simplified deployment and use scenarios made possible by smart card Plug and Play PIV support. Users will appreciate the ability to use smart cards to perform critical business tasks in a secure manner.

What are the benefits of the new and changed features?

The new smart card support options in Windows 7 include:

- **Encrypting drives with BitLocker Drive Encryption.** In the Windows 7 Enterprise and Windows 7 Ultimate operating systems, users can choose to encrypt their removable media by turning on BitLocker and then choosing the smart card option to unlock the drive. At run time, Windows retrieves the correct minidriver for the smart card and allows the operation to complete.
- **Smart card domain logon by using the PKINIT protocol.** In Windows 7, the correct minidriver for a smart card is retrieved automatically, enabling a new smart card to authenticate to the domain without requiring the user to install or configure additional middleware.
- **Document and e-mail signing.** Windows 7 users can rely on Windows to retrieve the correct minidriver for a smart card at run time to sign an e-mail or document. In addition, XML Paper Specification (XPS) documents can be signed without the need for additional software.

- **Use with line-of-business applications.** In Windows 7, any application that uses Cryptography Next Generation (CNG) or CryptoAPI to enable the application to use certificates can rely on Windows to retrieve the correct minidriver for a smart card at run time so that no additional middleware is needed.

What's the impact of these changes on smart card usage?

Smart card usage is expanding rapidly. To encourage more organizations and users to adopt smart cards for enhanced security, the process to provision and use new smart cards is simplified and supports more end user scenarios.

What's New in User Account Control

What's new in User Account Control?

Before the introduction of User Account Control (UAC), when a user was logged on as an administrator, that user was automatically granted full access to all system resources. While running as an administrator enabled a user to install legitimate software, the user could also unintentionally or intentionally install a malicious program. A malicious program installed by an administrator can fully compromise the computer and affect all users.

With the introduction of UAC, the access control model changed to help mitigate the impact of a malicious program. When a user attempts to start an administrator task or service, the **User Account Control** dialog box asks the user to click either **Yes** or **No** before the user's full administrator access token can be used. If the user is not an administrator, the user must provide an administrator's credentials to run the program. Because UAC requires an administrator to approve application installations, unauthorized applications cannot be installed automatically or without the explicit consent of an administrator.

In Windows® 7 and Windows Server® 2008 R2, UAC functionality is improved to:

- Increase the number of tasks that the standard user can perform that do not prompt for administrator approval.
- Allow a user with administrator privileges to configure the UAC experience in the Control Panel.
- Provide additional local security policies that enable a local administrator to change the behavior of the UAC messages for local administrators in Admin Approval Mode.
- Provide additional local security policies that enable a local administrator to change the behavior of the UAC messages for standard users.

Who will want to use UAC?

UAC helps standard users and administrators protect their computers by preventing programs that may be malicious from running. The improved user experience makes it easier for users to perform daily tasks while protecting their computers.

UAC helps enterprise administrators protect their network by preventing users from running malicious software.

What are the benefits of the new and changed features?

By default, standard users and administrators access resources and run applications in the security context of standard users. When a user logs on to a computer, the system creates an access token for that user. The access token contains information about the level of access that the user is granted, including specific security identifiers (SIDs) and Windows privileges.

When an administrator logs on, two separate access tokens are created for the user: a standard user access token and an administrator access token. The standard user access token contains the same user-specific information as the administrator access token, but the administrative Windows privileges and SIDs have been removed. The standard user access token is used to start applications that do not perform administrative tasks (standard user applications).

When the user runs applications that perform administrative tasks (administrator applications), the user is prompted to change or "elevate" the security context from a standard user to an administrator, called Admin Approval Mode. In this mode, the administrator must provide approval for applications to run on the secure desktop with administrative privileges. The improvements to UAC in Windows 7 and Windows Server 2008 R2 result in an improved user experience when configuring and troubleshooting your computer.

The built-in Administrator account in Windows Server 2008 R2 does not run in Admin Approval Mode
The built-in Administrator account in Windows Server 2008 R2, which is the first account created on a server, does not run in Admin Approval Mode. All subsequently created administrator accounts in Windows Server 2008 R2 do run in Admin Approval Mode.

The built-in Administrator account is disabled by default in Windows 7
The built-in Administrator account is disabled by default in Windows 7. The built-in Administrator account, by default, cannot log on to the computer in Safe Mode.

Behavior of computers that are not domain members
When there is at least one configured local administrator account, the disabled built-in Administrator account cannot log on in Safe Mode. Instead, any local administrator account can be used to log on. If the last local administrator account is inadvertently demoted, disabled, or deleted, Safe Mode allows the disabled built-in Administrator account to log on for disaster recovery.

If the built-in Administrator account is the only administrator account on Windows Vista, when upgrading to Windows 7, Safe Mode allows the disabled built-in Administrator account to log on to create at least one administrator account.

Behavior of computers that are domain members
The disabled built-in Administrator account in all cases cannot log on in Safe Mode. A user account that is a member of the **Domain Admins** group can log on to the computer to create a local administrator if none exists.

Important

If the domain administrator account has never logged on to the client computer, you must start the computer in Safe Mode with Networking to cache the credentials on the client computer.

Note

After the computer is removed from the domain, it reverts back to the non-domain member behavior.

All subsequent user accounts are created as standard users in Windows 7
Standard user accounts and administrator user accounts can use UAC enhanced security. In new Windows 7 installations, by default, the first user account created is a local administrator account in Admin Approval Mode (UAC enabled). All subsequent accounts are then created as standard users.

Reduced number of UAC prompts
Windows 7 and Windows Server 2008 R2 reduce the number of UAC prompts that local administrators and standard users must respond to.

To reduce the number of prompts that a local administrator must respond to:

- File operation prompts are merged.
- Internet Explorer prompts for running application installers are merged.
- Internet Explorer prompts for installing ActiveX® controls are merged.

The default UAC setting allows a standard user to perform the following tasks without receiving a UAC prompt:

- Install updates from Windows Update.
- Install drivers that are downloaded from Windows Update or included with the operating system.

- View Windows settings. (However, a standard user is prompted for elevated privileges when changing Windows settings.)
- Pair Bluetooth devices to the computer.
- Reset the network adapter and perform other network diagnostic and repair tasks.

Configure UAC experience in Control Panel
Windows Vista® offers two levels of UAC protection to the user: on or off. Windows 7 and Windows Server 2008 R2 introduce additional prompt levels that are similar to the Internet Explorer security zone model. If you are logged on as a local administrator, you can enable or disable UAC prompts, or choose when to be notified about changes to the computer. There are four levels of notification to choose from:

- **Never notify me**. You are not notified of any changes made to Windows settings or when software is installed.
- **Only notify me when programs try to make changes to my computer**. You are not notified when you make changes to Windows settings, but you do receive notification when a program attempts to make changes to the computer.
- **Always notify me**. You are notified when you make changes to Windows settings and when programs attempt to make changes to the computer.
- **Always notify me and wait for my response**. You are prompted for all administrator tasks on the secure desktop. This choice is similar to the current Windows Vista behavior.

The following table compares the number of UAC prompts for user actions in Windows 7 and Windows Server 2008 R2 with the number of UAC prompts in Windows Vista Service Pack 1.

Actions	Only notify me when programs try to make changes to my computer	Always notify me
Change personalization settings	No prompts	Fewer prompts
Manage your desktop	No prompts	Fewer prompts
Set up and troubleshoot your network	No prompts	Fewer prompts
Use Windows Easy Transfer	Fewer prompts	Same number of prompts
Install ActiveX controls through Internet Explorer	Fewer prompts	Fewer prompts
Connect devices	No prompts	No prompts if drivers are on Windows Update, or similar number of prompts if drivers are not on

		Windows Update
Use Windows Update	No prompts	No prompts
Set up backups	No prompts	Same number of prompts
Install or remove software	No prompts	Fewer prompts

Change the behavior of UAC messages for local administrators
If you are logged on as a local administrator, you can change the behavior of UAC prompts in the local security policies for local administrators in Admin Approval Mode.

- **Elevate without prompting**. Applications that are marked as administrator applications and applications that are detected as setup applications are run automatically with the full administrator access token. All other applications are automatically run with the standard user token.

- **Prompt for credentials on the secure desktop**. The **User Account Control** dialog box is displayed on the secure desktop. To give consent for an application to run with the full administrator access token, the user must enter administrative credentials. This setting supports compliance with Common Criteria or corporate policies.

- **Prompt for consent on the secure desktop**. The **User Account Control** dialog box is displayed on the secure desktop. To give consent for an application to run with the full administrator access token, the user must click **Yes** or **No** on the **User Account Control** dialog box. If the user is not a member of the local **Administrators** group, the user is prompted for administrative credentials. This setting supports compliance with Common Criteria or corporate policies.

- **Prompt for credentials**. This setting is similar to **Prompt for credentials on the secure desktop**, but the **User Account Control** dialog box is displayed on the desktop instead.

- **Prompt for consent**. This setting is similar to **Prompt for consent on the secure desktop**, but the **User Account Control** dialog box is displayed on the desktop instead.

- **Prompt for consent for non-Windows binaries**. The **User Account Control** dialog box is displayed on the desktop for all files that are not digitally signed with the Windows digital certificate.

Change the behavior of UAC messages for standard users
If you are logged on as a local administrator, you can change the behavior of UAC prompts in the local security policies for standard users.

- **Automatically deny elevation requests**. Administrator applications cannot run. The user receives an error message that indicates a policy is preventing the application from running.

- **Prompt for credentials**. This is the default setting. For an application to run with the full administrator access token, the user must enter administrative credentials in the **User Account Control** dialog box that is displayed on the desktop.

- **Prompt for credentials on the secure desktop**. For an application to run with the full administrator access token, the user must enter administrative credentials in the **User Account Control** dialog box that is displayed on the secure desktop.

What's the impact of these changes on UAC?

In response to customer requests, the improved UAC allows users to perform their daily tasks with fewer prompts and gives administrators more control over how UAC prompts users.

Because of the changes to UAC, when upgrading from Windows Vista to Windows 7, UAC settings are not transferred.

What's New in Windows Security Auditing

What are the major changes?

There are a number of auditing enhancements in Windows Server® 2008 R2 and Windows® 7 that increase the level of detail in security auditing logs and simplify the deployment and management of auditing policies. These enhancements include:

- **Global Object Access Auditing.** In Windows Server 2008 R2 and Windows 7, administrators can define computer-wide system access control lists (SACLs) for either the file system or registry. The specified SACL is then automatically applied to every single object of that type. This can be useful both for verifying that all critical files, folders, and registry settings on a computer are protected, and for identifying when an issue with a system resource occurs.

- **"Reason for access" reporting.** This list of access control entries (ACEs) provides the privileges on which the decision to allow or deny access to the object was based. This can be useful for documenting the permissions, such as group memberships, that allow or prevent the occurrence of a particular auditable event.

- **Advanced audit policy settings.** These 53 new settings can be used in place of the nine basic auditing settings under **Local Policies\Audit Policy** to allow administrators to more specifically target the types of activities they want to audit and eliminate the unnecessary auditing activities that can make audit logs difficult to manage and decipher.

The following sections describe these enhancements in greater detail.

What do these auditing enhancements do?

In Windows XP, administrators have nine categories of security auditing events that they can monitor for success, failure, or both success and failure. These events are fairly broad in scope and can be triggered by a variety of similar actions, some of which can generate a large number of event log entries.

In Windows Vista® and Windows Server 2008, the number of auditable events is expanded from nine to 53, which enables an administrator to be more selective in the number and types of events to audit. However, unlike the nine basic Windows XP events, these new audit events are not integrated with Group Policy and can only be deployed by using logon scripts generated with the Auditpol.exe command-line tool.

In Windows Server 2008 R2 and Windows 7, all auditing capabilities have been integrated with Group Policy. This allows administrators to configure, deploy, and manage these settings in the Group Policy Management Console (GPMC) or Local Security Policy snap-in for a domain, site, or organizational unit (OU). Windows Server 2008 R2 and Windows 7 make it easier for IT professionals to track when precisely defined, significant activities take place on the network.

Audit policy enhancements in Windows Server 2008 R2 and Windows 7 allow administrators to connect business rules and audit policies. For example, applying audit policy settings on a domain or OU basis will allow administrators to document compliance with rules such as:

- Track all group administrator activity on servers with finance information.
- Track all the files that are accessed by defined groups of employees.
- Confirm that the correct SACL is applied to every file, folder, and registry key when they are accessed.

Who will be interested in this feature?

Auditing enhancements in Windows Server 2008 R2 and Windows 7 support the needs of IT professionals who are responsible for implementing, maintaining, and monitoring the ongoing security of an organization's physical and information assets.

These settings can help administrators answer questions such as the following:

- Who is accessing our assets?
- What assets are they accessing?
- When and where did they access them?
- How did they obtain access?

Security awareness and the desire to have a forensic trail are significant motivators behind these questions. The quality of this information is required and evaluated by auditors in a growing number of organizations.

Are there any special considerations?

A number of special considerations apply to various tasks associated with auditing enhancements in Windows Server 2008 R2 and Windows 7:

- **Creating an audit policy.** To create an advanced Windows security auditing policy, you must use the GPMC or Local Security Policy snap-in on a computer running Windows Server 2008 R2 or Windows 7. (You can use the GPMC on a computer running Windows 7 after installing the Remote Server Administration Tools.)
- **Applying audit policy settings.** If you are using Group Policy to apply the advanced audit policy settings and global object access settings, client computers must be running Windows Server 2008 R2 or Windows 7. In addition, only computers running Windows Server 2008 R2 or Windows 7 can provide "reason for access" reporting data.
- **Developing an audit policy model.** To plan advanced security audit settings and global object access settings, you must use the GPMC targeting a domain controller running Windows Server 2008 R2.
- **Distributing the audit policy.** After a Group Policy object (GPO) that includes advanced security auditing settings has been developed, it can be distributed by using domain controllers running any Windows server operating system. However, if you cannot put client computers running Windows 7 in a separate OU, you should use Windows Management Instrumentation (WMI) filtering to ensure that the advanced policy settings are applied only to client computers running Windows 7.

Chapter 18 – What's New in the Server Core Installation Option

Chapter 18

What are the major changes?

The Windows Server® 2008 R2 operating system eases the task of managing and securing multiple server roles in an enterprise with enhancements to Server Manager.

The following functionality additions have been made to Server Manager in Windows Server 2008 R2:

- **Remote Management with Server Manager.** In Windows Server 2008 R2, you can use Server Manager to perform some management tasks on remote computers that are running Windows Server 2008 R2. To manage a computer remotely by using Server Manager, you connect Server Manager to a remote computer in the same manner you would connect the Microsoft Management Console (MMC) for other technologies.

  You can also create a custom MMC that contains multiple Server Manager snap-ins, each targeted to manage a different remote computer.

- **Best Practices Analyzer.** Best Practices Analyzer (BPA) is a server management tool that is available for a limited set of roles that run on Windows Server 2008 R2. Best Practices Analyzer can help administrators reduce best practice violations by scanning one or more roles that are installed on Windows Server 2008 R2, and reporting best practice violations to the administrator. Administrators can filter or exclude results from BPA reports that they do not need to see. Administrators can also perform BPA tasks by using either the Server Manager GUI, or Windows PowerShell™ cmdlets. Best Practices Analyzer is one of the areas of the **Summary** section of a role's home page.

- **Windows PowerShell cmdlets for Server Manager tasks.** The following three Windows PowerShell cmdlets allow you to install, remove, or view information about available roles by using Windows PowerShell. For more information about how to use any of these cmdlets, in a Windows PowerShell session, enter **Get-Help***cmdlet_name***–full**, in which *cmdlet_name* represents one of the following values.

  - **Add-WindowsFeature**
  - **Get-WindowsFeature**
  - **Remove-WindowsFeature**

- **Changes to roles and features available.** Windows Server 2008 R2 includes the following changes to roles and features that are available for installation by using Server Manager.
  - Roles
    - Terminal Services is now named Remote Desktop Services.
    - Windows Server Update Services (WSUS) is now available with Windows Server 2008 R2. In Windows Server 2008, WSUS is available as a separate package for downloading from the Microsoft Download Center (http://go.microsoft.com/fwlink/?LinkId=137379).
    - Print Services is now named Print and Document Services.
    - Universal Description, Discovery, and Integration (UDDI) Services is no longer available for installation on Windows Server 2008 R2 by using Server Manager.
  - Features
    - Windows BranchCache, a feature that is new for Windows Server 2008 R2, helps reduce the network bandwidth requirements of client computers that are located in remote offices.
    - Direct Access Management Console, a feature that provides direct access setup and monitoring capability, has been added for Windows Server 2008 R2.
    - Ink and Handwriting Services, new for Windows Server 2008 R2, provides support for both handwriting recognition and the use of a pen or stylus with a computing surface, such as a tablet computer.
    - Remote Server Administration Tools now includes Active Directory® Administrative Center, Remote Desktop (RD) Connection Broker tools, and BitLocker Recovery Password Viewer. The Windows® 7 version of Remote Server Administration Tools available for download on the Microsoft Download CenterConnect Web site includes the Server Manager console, which administrators can use to manage remote computers that are running Windows Server 2008 R2.
    - Windows 2000 Client Support has been removed from Message Queuing.
    - Windows Biometric Framework allows the use of fingerprint-reading devices on a computer to verify the identities of users.
    - Windows Server Migration Tools lets an administrator migrate some server roles, features, operating system settings, shares, and other data from computers that are running certain editions of Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2 to computers that are running Windows Server 2008 R2. Windows Remote Management (WinRM) IIS Extension enables a server to receive a remote management request from a client by using the WS-Management protocol.
    - XPS Viewer, part of .NET Framework 3.0 Features in Windows Server 2008, is available in Windows Server 2008 R2 as a stand-alone feature.

What does Server Manager do?

Server Manager, first available in the Windows Server 2008 operating system, provides a single source for managing a server's identity and system information, displaying server status, identifying problems with server role configuration or the alignment of some roles to best practices, and managing all roles installed on the server. With the release of Windows Server 2008 R2, Server Manager can be used to manage remote computers, either from another computer that is running Windows Server 2008 R2, or a computer that is running Windows 7.

Who will be interested in Server Manager?

Server Manager provides the greatest benefit to any of the following IT professionals:

- An IT administrator, planner, or analyst who is evaluating Windows Server 2008 R2.
- An enterprise IT planner or designer.
- An early adopter of Windows Server 2008 R2.
- An IT architect who is responsible for computer management and security throughout an organization.
- An IT administrator whose duties include server configuration, deployment, security hardening, or best practice compliance.

Are there any special considerations?

Whether you are running Server Manager on a local computer, or you are running a Server Manager console that is targeted at a remote computer, you must be a member of the **Administrators** group on the computer that you are managing.

The following are other considerations and requirements for using the new Server Manager functionality.

Special considerations for running Best Practices Analyzer

- For this release, you can perform Best Practices Analyzer scans on the following roles. Before you can run a scan, you must install on the computer the roles that you want to scan.
    - Active Directory Domain Services
    - Active Directory Certificate Services
    - Domain Name System (DNS) Server
    - Remote Desktop Services
    - Web Server (IIS)
- To scan multiple roles at one time, you must run a Best Practices Analyzer scan by using Windows PowerShell cmdlets. Special considerations for remote management with Server Manager
- Whether you use Server Manager to manage remote computers from a computer that is running Windows 7 or Windows Server 2008 R2, remote management by using Server Manager requires several command-line configuration steps before the remote computer gives users connections. Additionally, on the remote computer that is running Windows Server 2008 R2, the **Allow remote management of this server from**

other computers by using Server Manager and Windows PowerShell option must be selected. Although the Server Manager console cannot run on the Server Core installation option of Windows Server 2008 R2, you can use Windows PowerShell cmdlets on the Server Core installation option, after you install Windows PowerShell on the Server Core installation option. You can manage remote computers that are running the Server Core installation option of Windows Server 2008 R2 with the Server Manager console that is available on the full installation option, if you are a member of the **Administrators** group on the computer that is running the Server Core installation option.

Special considerations for using Windows PowerShell cmdlets for Server Manager tasks

- To run any Server Manager–related Windows PowerShell cmdlets on Windows Server 2008 R2, including Windows Server Migration Tools and Best Practices Analyzer cmdlets, you must be running Windows PowerShell with elevated user rights. To do this, click **Start**, click **All Programs**, click **Accessories**, click **Windows PowerShell**, right-click the Windows PowerShell shortcut, and then click **Run as administrator**.

- You must load the Server Manager module into each new Windows PowerShell session before working with Server Manager cmdlets. To do this, in a Windows PowerShell session opened with elevated user rights, type **Import-Module Servermanager**, and then press ENTER.

- To perform Best Practices Analyzer scans by using Windows PowerShell cmdlets, in addition to loading the Server Manager module into your Windows PowerShell session, you must also load the Best Practices Analyzer module

Chapter 19 – What's New in Server Manager

What are the major changes?

The Server Core installation option of Windows Server® 2008 R2 includes support for additional server roles and features. Server Core installations of Windows Server 2008 R2 now use the Deployment Image Servicing and Management (DISM) tool to install and uninstall server roles.

The following changes are available in Windows Server 2008 R2:

- In addition to the server roles available in Server Core installations of Windows Server® 2008, the following are available:
  - The Active Directory® Certificate Services (AD CS) role
  - The File Server Resource Manager component of the File Services role
  - A subset of ASP.NET in the Web Server role
- In addition to the Windows features available in Server Core installations of Windows Server 2008, the following features are available:
  - .NET Framework
    - A subset of .NET Framework 2.0
    - A subset of .NET Framework 3.0, including Windows Communication Foundation (WCF) and Windows Workflow Foundation (WF)
    - A subset of .NET Framework 3.5, including WF additions from .NET Framework 3.5 and .NET Language-Integrated Query (LINQ)
  - Windows PowerShell, including cmdlets for Server Manager and the Best Practices Analyzer
  - Windows-on-Windows 64-bit (WoW64)
- The Removable Storage feature has been removed.
- You can remotely configure a server running a Server Core installation of Windows Server 2008 R2 by using Server Manager.

Who will be interested in this feature?

The Server Core installation option provides a minimal environment for running specific server roles. Because it installs only the subset of binary files that are required by the supported server roles, this installation option reduces the maintenance and management requirements, as well as the attack surface for those server roles.

The following groups might be interested in these changes:

- IT planners, analysts, and designers
- IT professionals who are managing any of the supported server roles
- Developers and persons who design, develop, and host Web servers

Chapter 20 – What's New in the Web Server (IIS) Role (IIS 7)

Chapter 20

What are the major changes?

Many features have been added or enhanced in Internet Information Services (IIS) 7.5, which is the foundation of the Web Server role in Windows Server® 2008 R2.

The following changes are available in the Web Server (IIS) role in Windows Server 2008 R2:

- Integrated extensions
  - WebDAV and FTP
  - Request Filtering
  - Administration Pack modules
- Management enhancements
  - Best Practices Analyzer
  - Windows PowerShell™ Provider and cmdlets
  - Configuration logging and tracing
- Application hosting enhancements
  - Service hardening
  - Managed service accounts
  - Hostable Web Core
  - Failed Request Tracing for FastCGI
- Enhancements to .NET support on Server Core

Integrated extensions

Building on the extensible and modular architecture introduced with IIS 7.5, the new IIS 7.5 integrates and enhances existing extensions while still providing additional extensibility and customization.

WebDAV and FTP
WebDAV and FTP functionality available in IIS 7 has been greatly enhanced by incorporating many new features that enable Web authors to publish content more reliably and securely than before. The new FTP and WebDAV modules also offer Web server administrators more options for authentication, auditing, and logging.

Request Filtering
The Request Filtering module, previously available as an extension for IIS 7, helps prevent potentially harmful requests from reaching the server by allowing you to restrict or block specific HTTP requests.

Administration Pack modules
Extension modules previously available for IIS 7 as part of the IIS Administration Pack offer additional tools to help you administer your IIS 7.5 Web server from IIS Manager. These modules include the Configuration Editor and UI extensions that will help you manage Request Filtering rules, FastCGI, and ASP.NET application settings.

Management enhancements

IIS 7.5 has the same distributed and delegated management architecture as IIS 7, but IIS 7.5 also offers new administration tools.

Best Practices Analyzer
Best Practices Analyzer (BPA) is a management tool that can be accessed by using Server Manager and Windows PowerShell. BPA can help administrators reduce best practice violations by scanning an IIS 7.5 Web server and reporting when potential configuration issues are found.

Windows PowerShell Provider and cmdlets
The IIS module for Windows PowerShell is a Windows PowerShell snap-in that allows you to perform IIS administrative tasks and manage IIS configuration and run-time data. In addition, a collection of task-oriented cmdlets provide a simple way to manage Web sites, Web applications, and Web servers.

Configuration logging and tracing
Configuration logging and tracing allows you to audit access to the IIS configuration and to track successful or failed modifications by enabling any new logs that become available in the Event Viewer.

Application hosting enhancements

Offering a variety of new features that help increase security and improve diagnostics, IIS 7.5 is an even more flexible and manageable platform for many types of Web applications, such as ASP.NET and PHP.

Service hardening
Building on the IIS 7 application pool isolation model that increased security and reliability, every IIS 7.5 application pool now runs each process as a unique, less-privileged identity.

Managed service accounts
Domain accounts that have passwords managed by the host computer are now supported as service identities in IIS 7.5. This means that server administrators no longer have to worry about expiring application pool passwords.

Hostable Web Core
Core IIS Web engine components can be consumed or hosted by other applications. This lets IIS components service HTTP requests directly in an application. This is useful for enabling basic Web server capabilities for custom applications or for debugging applications.

Failed Request Tracing for FastCGI
In IIS 7.5, PHP developers that use the FastCGI module can implement IIS trace calls within their applications. Developers can then troubleshoot application errors by using IIS Failed Request Tracing to debug the code during development.

Enhancement to .NET support on Server Core

The Server Core installation option of Windows Server 2008 R2 provides support for the .NET Framework 2.0, 3.0, 3.5.1, and 4.0. This means you can host ASP.NET applications, perform remote management tasks from IIS Manager, and locally run cmdlets included with the Windows PowerShell Provider for IIS.

Chapter 21 – What's New in Windows Deployment

Chapter 21

What are the major changes?

The following changes to Windows Deployment Services are available in Windows Server 2008 R2:

- **Dynamic driver provisioning**. The ability to deploy driver packages to client computers as part of an installation, and the ability to add driver packages to boot images prior to deployment. For details, see Driver package provisioning later in this topic.
- **Virtual hard disk deployment**. The ability to deploy virtual hard disk (.vhd) images as part of an unattended installation. For details, see .vhd deployment later in this topic.
- **Additional multicasting functionality**. The ability to automatically disconnect slow clients and divide transmissions into multiple streams based on client speeds. Also provides support for multicasting in environments that use IPv6.
- **PXE provider for Transport Server**. Includes a PXE provider when you install the Transport Server role service. You can use Transport Server to network boot, multicast data, or both as part of an advanced configuration. Transport Server is a stand-alone server. That is, when you use Transport Server for network booting and multicasting, your environment does not need Active Directory Domain Services (AD DS) or Domain Name System (DNS). For instructions, see the Configuring Transport Server topic.
- **Additional EFI functionality**. Supports network booting of x64-based computers with EFI, including Auto-add functionality, DHCP referral to direct clients to a specific PXE server, and the ability to deploy boot images by using multicasting.

Dynamic driver provisioning
In Windows Server 2008 R2, you can add and configure driver packages on a server that is running Windows Deployment Services. After you have added the driver packages to the server, you can do the following:

- Deploy driver packages to client computers based on the hardware of the client as part of an installation.

> **Note**
>
> This functionality is only available when you are installing images of the following operating systems: Windows Vista with SP1, Windows Server 2008, Windows 7, and Windows Server 2008 R2.

- Add driver packages (such as network adapter drivers, mass storage drivers, and bus drivers) to your Windows 7 and Windows Server 2008 R2 boot images.

Why is this change important?
This new functionality provides the following benefits:

- Eliminates the need to add driver packages manually by using the tools in the Windows Automated Installation Kit.
- Minimizes the size of install images.
- Makes it easier to update and manage drivers because the drivers are stored outside the images.
- Eliminates the need to maintain multiple images for different hardware configurations.
- Eliminates the need for additional tools to manage drivers (for example, the Microsoft Deployment Toolkit (MDT) or non-Microsoft solutions).
- Eliminates the need to use an Unattended installation file to add drivers.

How should I prepare for this change?
The following are prerequisites for driver package provisioning:

- A Windows Deployment Services server that is configured with the following:
  - The boot image from Windows 7 or Windows Server 2008 R2 (from \Sources\Boot.wim on the installation DVD).
  - Install images for Windows Vista SP1, Windows Server 2008, Windows 7, or Windows Server 2008 R2.
- Driver packages for the hardware that you want to deploy. Note that these packages must be extracted (that is, the package cannot be a .msi or .exe file).

Virtual hard disk deployment
You can deploy .vhd images of Windows Server 2008 R2 to a physical computer (not a virtual machine) by using Windows Deployment Services. In general, you deploy .vhd images in the same way that you deploy .wim images. This scenario is intended for advanced users who already have .vhd images.

Why is this change important?
This new functionality provides the following benefits:

- Allows you to standardize .vhd as your common image format. Previously, you had to manage operating system images in the .vhd format for virtual machines and in the .wim format for physical computers.
- Simplifies image deployment by enabling physical computers to boot from .vhd images.
- Allows you to provision a server with multiple .vhd images and switch between the images with ease. You can create multiple .vhd images that are customized for different roles and deploy them all to a single server. Then, if the balance of workloads changes in the data center (for example, you want to reallocate a computer running Microsoft SQL Server to be a Web server), you can boot into the .vhd for that role instead of reinstalling the operating system.
- Allows you to roll back changes when you use differencing disks.

What works differently?
Using WDSUTIL at the command line is the only supported method of adding and configuring the images. In addition, the deployment must be part of an automated installation, so you must create and configure two unattend files to automate the installation

Chapter 22 – What's New in Windows Deployment Services

Chapter 22

What are the major changes?

New versions of Windows Deployment Services, the Windows® Automated Installation Kit (Windows AIK), and the Microsoft Deployment Toolkit (MDT) are available to assist in the deployment of Windows® 7 and Windows Server® 2008 R2. Each of these tools includes new features that improve the process of deploying Windows.

The following list describes the different Windows deployment technologies and the major changes for deployment in this release:

- **Microsoft Deployment Toolkit**

  The Microsoft Deployment Toolkit (MDT) is a solution accelerator that collects many Microsoft deployment technologies together into a single means of automating installations. Using MDT, you can automate Windows operating-system installations by using Zero Touch Installation (ZTI) or Lite Touch Installation (LTI) processes. The deployment of Windows can be completely automated by using the ZTI method, or require a minimum of interaction at the targeted computer by using the LTI method. ZTI uses Microsoft System Center Configuration Manager 2007 or Microsoft Systems Management Server 2003 with the Operating System Deployment Feature Pack.

- **Windows Deployment Services**

  Windows Deployment Services is a server role that was included with Windows Server® 2008; it has been updated for Windows Server 2008 R2. This version contains new multicast features and driver-provisioning functionality. With driver provisioning, you can deploy driver packages (along with a Windows image) to client computers based on the hardware of the client, and add driver packages to boot images.

  This version also enables you to deploy virtual hard disk (VHD) images by using an unattended installation.

- **Windows Automated Installation Kit**

  The Windows Automated Installation Kit (Windows AIK) is a collection of tools and documentation that enable you to customize your own Windows deployment environment. This collection of tools includes all of the Windows Setup configuration options, imaging tools, Windows Preinstallation Environment customizations, and processes and guidance. The Windows AIK is ideal for highly customized deployment environments and provides extensive control and flexibility.

Chapter 23 – What's New in Windows PowerShell

What are the major changes?

The following changes are available in Windows PowerShell in Windows Server 2008 R2:

- **New cmdlets.** Windows PowerShell includes more than 100 new cmdlets, including Get-Hotfix, Send-MailMessage, Get-ComputerRestorePoint, New-WebServiceProxy, Debug-Process, Add-Computer, Rename-Computer, and Reset-ComputerMachinePassword.

- **Remote management.** You can run commands on one computer or on hundreds of computers by using a single command. You can establish an interactive session with a single computer, or you can establish a session that can receive remote commands from multiple computers.

- **Windows PowerShell Integrated Scripting Environment (ISE).** Windows PowerShell ISE is a graphical user interface for Windows PowerShell that lets you run commands and write, edit, run, test, and debug scripts in the same window. It offers up to eight independent execution environments and includes a built-in debugger, multiline editing, selective execution, syntax colors, line and column numbers, and context-sensitive Help. Windows PowerShell ISE is an optional feature of Windows Server 2008 R2. To install it, use the Add Features Wizard.

- **Background jobs.** With Windows PowerShell background jobs, you can run commands asynchronously and "in the background" so you can continue to work in your session. You can run background jobs on a local or remote computer, and you can store the results locally or remotely.

- **Debugger.** The Windows PowerShell debugger can help you debug functions and scripts. You can set and remove breakpoints, step through code, check the values of variables, and display a call-stack trace.

- **Modules.** Windows PowerShell modules let you organize your Windows PowerShell scripts and functions into independent, self-contained units. You can package your cmdlets, providers, scripts, functions, and other files into modules that you can distribute to other users. Modules are easier for users to install and use than Windows PowerShell snap-ins. Modules can include any type of file, including audio files, images, Help files, and icons. Modules run in a separate session to avoid name conflicts.

- **Transactions.** Windows PowerShell now supports transactions, which let you manage a set of commands as a logical unit. A transaction can be committed, or it can be completely undone so that the affected data is not changed by the transaction.

- **Events.** Windows PowerShell includes a new event infrastructure that lets you create events, subscribe to system and application events, and then listen, forward, and act on the events synchronously and asynchronously.

- **Advanced functions.** Advanced functions behave just like cmdlets, but are written in the Windows PowerShell scripting language instead of in C#.

- **Script internationalization.** Scripts and functions can display messages and Help text to users in multiple languages.

- **Online Help.** In addition to Help at the command line, the Get-Help cmdlet has a new Online parameter that opens a complete and updated version of each Help topic on Microsoft TechNet.

Chapter 24 – What's New in Windows Search, Browse, and Organization

What's new in Windows Search, Browse, and Organization?

Windows® 7 introduces a number of new features and enhancements that can help IT professionals deploy and maintain desktop search, browse, and organization functionality:

- Improvements in the performance and stability of the indexer.
- Improvements in the performance and relevance of the search experience.
- The introduction of federated search and search connectors.
- The introduction of aggregation and visualizations to improve the organization of search results.
- The introduction of libraries to help with organization.
- Improvements in the performance and user interface of Windows Explorer.
- Additional Group Policy settings, available on all supported operating systems.
- Reduced impact on the server running Microsoft Exchange Server when indexing uncached (classic online) e-mail.
- The ability to index delegate mailboxes for e-mail.
- Support for indexing encrypted documents of local file systems.
- Support for indexing digitally signed e-mail of MAPI-enabled e-mail clients such as Microsoft Outlook®.
- An expanded ability to do fast remote queries of file shares, including on Windows Vista®, Windows Server® 2008, Windows® XP with Windows Search 4.0 installed, and earlier versions.

The Windows Search Service enables you to perform fast file searches on a server from computers running Windows 7 or Windows Server® 2008 R2, or from computers that have Windows Desktop Search installed and are running Windows Vista, Windows Server 2008, Windows XP, Windows Server® 2003 R2, or Windows Server® 2003.

Note

Indexing of uncached e-mail is also known as classic online e-mail. In Windows® 7, there is less impact on Microsoft Exchange Server when indexing uncached e-mail. In contrast to uncached or classic online e-mail, cached e-mail uses a local Offline Folder file (.ost) to keep a local copy of your Exchange Server mailbox on your computer, which permits indexing of e-mail locally.

Who will want to use Windows Search, Browse, and Organization?

This feature is intended for end users and IT professionals.

Before deploying Windows 7, administrators should consider several factors, including the following:

- The role of desktop search within your enterprise search strategy.
- Which data stores or services you want to publish for direct client access in Windows Explorer by using the OpenSearch standard.
- Current document storage practices and how they relate to libraries.
- The importance of file storage encryption to your organization.
- The importance of e-mail encryption and signing to your organization.

What are the benefits of the new and changed features?

A brief overview of the major new features and capabilities for Windows Search, Browse, and Organization in Windows 7 is provided in the following table.

Feature	New in Windows 7
Improvements in the performance and user interface of Windows Explorer	The navigation is better organized and more intuitive, everyday tasks are easier to access, and there are numerous improvements in the presentation of end user content.
The introduction of libraries to help with organization	Libraries make it quicker and easier to find files. Built on the existing **My Documents** experience, libraries work like folders do but have additional functionality. In addition to browsing files by using the hierarchical folder structure, you can also browse metadata such as date, type, author, and tags. Users can include files from multiple storage locations in their libraries without having to move or copy the files from original storage locations.
Improvements in the search experience	The search experience is integrated into everyday tasks through Windows Explorer, the **Start** menu, and the introduction of new libraries. Search results take relevance into account, making it faster to find what you are looking for. Other improvements to the experience include the introduction of highlighted matches in the searched document, a search builder to construct advanced queries, and arrangement views. Arrangement views allow you to pivot search results, list the most recent searches, and provide broader **Start** menu scope including Control Panel tasks.
The introduction of federated search and search connectors	Windows 7 enables searching for content on remote indices. Integrating federated search into Windows gives users the benefits of using familiar tools and workflows to search remote data. This enhanced integration provides the added benefit of highlighting matches within the searched document. Windows 7 enables federated search via the public OpenSearch standard. Other improvements are the consistent UI for remote search results within Windows Explorer and the ability to drag and drop files listed in the search results between different locations.

Indexing of uncached (classic online) e-mail	Before users can search for e-mail, the Windows indexing service must index the e-mail store, which involves collecting the properties and content of e-mail items within the store. This initial indexing is later followed by smaller incremental indexing (as e-mail arrives, is read, and deleted, and so on) to keep the index current. Windows 7 minimizes the impact on the server running Exchange Server by reducing the number of remote procedure calls (RPC) required to index e-mail messages and attachments. Because e-mail messages are indexed in native formats (HTML, RTF, and text) there is no load on the server to convert mail types. Windows indexes public folders only when they are cached locally.
Remote query	Windows 7 extends the ability to search across remote desktops. Windows 7 or Windows Search 4.0 (available on Windows Vista and Windows XP) enables users to query remote computers running on supported operating systems; Windows Vista allows users to search remote computers only if they are running Windows Vista.
Support for indexing encrypted files	Windows 7 fully supports indexing encrypted files on local file systems, allowing users to index and search the properties and contents of encrypted files. Users can manually configure Windows to include encrypted files in indexing, or administrators can configure this by using Group Policy.
Support for indexing digitally signed e-mail	Windows 7 allows users to search all content in digitally signed e-mail messages. This includes the message body and any attachments. A computer that is running Windows Vista Service Pack 1 (SP1) and Windows Search 4.0 functions as follows: • Users can search all digitally signed e-mail messages that they have sent. This search includes all message content. • Users can search all digitally signed e-mail messages that they have received. However, these searches are limited to certain properties, such as subject, sender, or recipients. Users cannot search the message body or attachment contents.

What's the impact of these changes?

There are significant improvements in how you search, browse, and organize in Windows 7:

- Closer integration with everyday workflows.
- More relevant search results.
- Highlighted search terms to easily identify results.
- An integrated advanced query builder.

In Windows 7, there is a new emphasis on organization with the introduction of libraries and the multiple improvements in the arrangement views and visualization of data.

Chapter 25 – What's New in Windows Server Backup

What are the major changes?

Windows Server Backup in Windows Server® 2008 R2 has been greatly enhanced and introduces features that allow for more control in what you can back up and where you can store backups. It also provides expanded command-line and Windows PowerShell™ support for managing backups remotely.

The following changes are available in Windows Server 2008 R2. These changes result in improved flexibility, efficiency, and manageability for creating and managing backups, and running recoveries:

- Ability to back up/exclude individual files and to include/exclude file types and paths from a volume
- Improved performance and use of incremental backups
- Expanded options for backup storage
- Improved options and performance for system state backups and recoveries
- Expanded command-line support
- Expanded Windows PowerShell support

For details about these changes, see the new functionality section later in this topic.

What does Windows Server Backup do?

Windows Server Backup consists of a Microsoft Management Console (MMC) snap-in, command-line tools, and a Windows PowerShell snap-in and cmdlets that provide a complete solution for your day-to-day backup and recovery needs. You can use Windows Server Backup to back up a full server (all volumes), selected volumes, the system state, or specific files or folders—and to create a backup that you can use for bare metal recovery. You can recover volumes, folders, files, certain applications, and the system state. And, in case of disasters like hard disk failures, you can perform a bare metal recovery. You can use Windows Server Backup to create and manage backups for the local computer or a remote computer. And, you can schedule backups to run automatically.

Who will be interested in this feature?

Windows Server Backup is intended for use by everyone who needs a basic backup solution—from small business to large enterprises.

The following groups might be interested in these changes:

- IT professionals responsible for infrastructure, backup, and disaster recovery
- Small businesses or individuals who are not IT professionals who are looking for an all-in-one, step-by-step backup solution

- Medium or large businesses looking for a flexible and efficient backup solution that can be scripted and managed remotely

Are there any special considerations?

To perform a bare metal or operating system recovery, you will need a backup (created using Windows Server Backup) of the full server or just the volumes that contain operating system files, and the Windows Recovery Environment—this will restore your complete system onto your old system or a new hard disk.

Certain backup or recovery tasks must be performed with two computers running the same version of Windows Server 2008 or Windows Server 2008 R2, while others may be performed with computers running either version. The following table shows the tasks that you can perform with a given type of backup.

	Backup created with Windows Server 2008	Volume backup created with Windows Server 2008 R2	File/folder backup created with Windows Server 2008 R2	Bare metal recovery backup created with Windows Server 2008
Perform a file/folder recovery for a computer running Windows Server 2008	Supported	Not supported	Not supported	Supported
Perform a volume recovery for a computer running Windows Server 2008	Supported	Not supported	Not supported	Supported
Perform a bare metal recovery for a computer running Windows Server 2008	Supported	Not supported	Not supported	Supported
Perform a system state recovery for a computer running Windows Server 2008	Supported	Not supported	Not supported	Supported
Manage backups with the **Wbadmin** command on a computer running Windows Server 2008	Supported	Not supported	Not supported	Supported
Manage backups with the Windows Server Backup MMC snap-in in Windows Server 2008	Supported	Not supported	Not supported	Supported
Manage backups with the Windows PowerShell cmdlets in	Supported	Not supported	Not supported	Supported

Windows Server 2008				
Perform remote backups or recoveries using the **Connect To Another Computer** option in Windows Server 2008 R2	Not supported	Supported	Supported	Not supported
Perform a file/folder recovery for a computer running Windows Server 2008 R2	Supported	Supported	Supported	Supported
Perform a volume recovery for a computer running Windows Server 2008 R2	Supported	Supported	Supported	Supported
Perform a bare metal recovery for a computer running Windows Server 2008 R2	Not supported	Supported	Supported	Not supported
Perform a system state recovery for a computer running Windows Server 2008 R2	Not supported	Supported	Supported	Not supported
Manage backups with the **Wbadmin** command for a computer running Windows Server 2008 R2	Supported	Supported	Supported	Supported
Manage backups with the Windows Server Backup user interface in Windows Server 2008 R2	Supported	Supported	Supported	Supported
Manage backups with the Windows PowerShell cmdlets in Windows Server 2008 R2	Supported	Supported	Supported	Supported

What new functionality does this feature provide?

Ability to back up/exclude individual files and to include/exclude file types and paths from a volume
Windows Server Backup enables you to back up selected files instead of just full volumes. In addition, you can exclude files from your backups based on file type or path.

Why is this change important?
This change offers you more flexibility and control in what you include in your backups, instead of requiring you to back up full volumes.

What works differently?
New options have been added to the Schedule Backup and Backup Once wizards (available in the Windows Server Backup snap-in). These options enable you to pick files and folders to add to your backup, and exclude file types and paths from your backup. In addition, the **Wbadmin enable backup** and **Wbadmin start backup** commands have been updated to include this functionality.

Improved performance and use of incremental backups
Windows Server Backup, by default, creates incremental backups that function like full backups (you can recover any item from a single backup, but the backup will only occupy space needed for an incremental backup). All file/folder backups (except the first one) are incremental backups where only the changed files are read and transferred to the backup storage location. In addition, Windows Server Backup does not require user intervention to periodically delete older backups to free disk space for newer backups—older backups are deleted automatically.

Why is this change important?
This change offers improved performance time to create backups that take up less space. In addition, because of this change, administrators do not need to delete older backups manually or do anything else to make sure unneeded backups are being deleted.

What works differently?
There is no user action required to create incremental backups. However, if you are backing up full volumes, you can configure performance settings by using the updated **Optimize Backup Performance** dialog box available from the Windows Server Backup MMC snap-in.

Expanded options for backup storage
You can now store backups created using a scheduled backup on a remote shared folder or volume. (If you store backups on a remote shared folder, only one version of your backup will be maintained.) You can also store backups on virtual hard disks.

Why is this change important?
This change enables you to store backups in locations that also contain other data—you no longer have to dedicate an entire disk for storing backups.

What works differently?
New options have been added to the Schedule Backup Wizard (available in the Windows Server Backup MMC snap-in) to select a remote shared folder or volume as the backup storage location. In addition, the **Wbadmin enable backup** command has been updated to include this functionality.

Improved options and performance for system state backups and recoveries
You can now use the Windows Server Backup MMC snap-in to create backups that you can use to perform system state recoveries. In addition, you can use a single backup to back up both the system state and other data on your server. These system state backups are now faster and require less space for multiple versions because they use shadow copies for versioning (similar to volume-based backups), and not individual folders for each version.

Why is this change important?
In Windows Server 2008, you could only create system state backups using the **Wbadmin** command. In addition, you could not back up the system state and other items in the same backup, which made performing recoveries more difficult.

What works differently?
New options have been added to the Schedule Backup and Backup Once wizards (available in the Windows Server Backup MMC snap-in) that enable you to create a backup of the system state and to add other items to the backup at the same time. In addition, the **Wbadmin enable backup** and **Wbadmin start backup** commands have been updated to include the parameter **–systemState**, which enables you to include the system state in a scheduled or one-time backup.

Expanded command-line support
Changes to **Wbadmin** command mirror the changes for the Windows Server Backup MMC snap-in—that is, the ability to back up files instead of full volumes, the ability to exclude certain file types or paths, and the ability to store scheduled backups on remote shared folders and volumes.

Why is this change important?
The changes to the **Wbadmin** command provide increased control, performance, and capabilities—and also keep the user interface and the command consistent with each other.

What works differently?
The functionality of following commands has been updated:

- **Wbadmin enable backup**
- **Wbadmin start backup**
- **Wbadmin start sysrecovery**

Expanded Windows PowerShell support
Windows Server Backup has enhanced the Windows PowerShell cmdlets in Windows Server 2008 R2 to automate routine tasks and better manage the backup scripts by using Windows PowerShell capabilities.

Why is this change important?
The changes provide improved management, remote management, and scripting capabilities—and also keep the cmdlet support consistent with changes made to the Windows Server Backup MMC snap-in and **Wbadmin** command.