

Comparison of Windows Server® 2003 and
Windows Server® 2008

Published: January 2008

© 2008 Microsoft Corporation. All rights reserved. This document is developed prior to the product’s release to manufacturing, and as such, we cannot guarantee that all details included herein will be exactly as what is found in the shipping product. The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication. The information represents the product at the time this document was printed and should be used for planning purposes only. Information subject to change at any time without prior notice. This whitepaper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

Microsoft, Active Directory, PowerShell, SharePoint, SoftGrid, Windows, Windows Media, the Windows logo, Windows Vista, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.





Table of Contents

Introduction 1

Improving Security 2

Network Access Protection (NAP) 2

Network Policy and Access Services (NPAS) Role 4

Server Core 5

Windows Firewall with Advanced Security 6

Read-Only Domain Controller (RODC) 7

Cryptography Next Generation (CNG) 8

Windows BitLocker Drive Encryption 9

Encrypting File System (EFS) 10

Federated Rights Management & Active Directory Rights Management Services 11

Virtualization 12

Terminal Services (TS) Presentation Virtualization 12

Virtualization through Hyper-V 12

Providing Remote Access 14

Terminal Services Role 14

Terminal Service Core Functionality 14

TS RemoteApp 16

TS Web Access 17

Terminal Services Gateway 17

Terminal Services Licensing 18

TS Session Broker 19

Active Directory Enhancements 20

Active Directory Domain Services Role 20

Active Directory Certificates Services Role 22

Active Directory Federation Services Role 23

Active Directory Lightweight Directory Services Role 24

Active Directory Rights Management Services Role (AD RMS) 25

Server Management Made Easier 26

Server Manager 26

Windows Reliability and Performance Monitor 27

Web Hosting 28

Internet Information Services (IIS) 29

Automating Tasks 30

Windows PowerShell 31

Application Enhancements 32

Windows Activation Service (WAS) 32

Application Server Role and Application Server Foundation 32

Better Together with Windows Vista 33

Remote Sites 35

Business Continuity 36

Next Generation TCP/IP Protocols and Networking Components 39

Interoperability 41

Conclusion 41

Comparison of Features in Windows Server 2003 and Windows Server 2008 43

References 51

# Introduction

The computing landscape has changed radically since the introduction of Microsoft® Windows Server® 2003. Windows Server® 2008 introduces many new features and extends the capabilities of Windows Server 2003. Windows Server 2008 is engineered to meet new security challenges, take advantage of new technologies, and provide a robust system that is easier to administer. To help organizations meet these challenges and to make administering systems easier for technical staff, many new features and technologies are introduced in Windows Server 2008 that were not available in Windows Server 2003 R2. Windows Server 2008 provides a wide range of benefits for organizations and IT staff in these areas:

* **Security**: The security of Windows Server 2008 is greatly enhanced by improving many existing capabilities and adding new features. Security enhancements are provided in features such as Network Access Protection (NAP), Windows® BitLocker™ Drive Encryption, Server Core, Cryptography Next Generation (CNG), Read-Only Domain Controller (RODC), and Windows Firewall with Advanced Security.
* **Virtualization:** In virtualization technology, Windows Server 2008 helps provide the ability to move disparate servers to Virtual Machines (VMs) in a centrally managed environment. Hyper-V™, the virtualization tool built into Windows Server 2008, allows organizations to consolidate servers and use hardware more efficiently.
* **Web:** Windows Server 2008 extends Web capabilities to help organizations deliver rich Web-based experiences efficiently and effectively, with improved administration and diagnostics, development and application tools, and lower infrastructure costs.
* **Solid foundation for business workloads:** Windows Server 2008 provides a versatile and reliable Windows platform for all of an organization’s workload and application requirements, giving administrators powerful, .new scripting, administration, configuration, and deployment features such as Server Manager in Windows Server 2008, Windows PowerShell, and Windows Deployment Services.
* **Remote Sites:** Windows Server 2008 includes many enhancements, and also has new features to make it easier to administer remote locations. Changes in the remote infrastructure in Windows Server 2008 make administration easier, improve security, and help increase productivity for personnel in remote sites by automating time-consuming tasks.

See the table later in this document for a comparison of features in Windows Server 2003 and Windows Server 2008.

## Improving Security

The security of Windows Server 2008 is greatly enhanced by having improved many existing capabilities and also adding new features. Windows Server 2008 installs only the services needed for the roles that the server is performing. Enhanced auditing, Windows® BitLocker™ Drive Encryption, and event forwarding are just some of the technologies that will help organization adhere to today's strict IT compliance standards. Organizations can secure their data and control network access Windows Server 2008. Network Access Protection (NAP) and Network Policy and Access Services (NPAS) roles help to regulate network access, while the new Windows Firewall with Advanced Security, Read-Only Domain Controllers (RODC), BitLocker Drive Encryption, and Cryptography Next Generation (CNG) can be used to help secure data. Windows Server 2008 Active Directory® Rights Management Services (AD RMS)—formerly Windows RMS—is a key to providing protection for sensitive information.

## Network Access Protection (NAP)

Organizations today have many mobile users who take mobile computers, such as laptops, from site to site, or users who connect to the network from home. Computers brought onsite or connecting from these uncontrolled environments can pose risks of spreading viruses or jeopardizing compliance. Network Access Protection (NAP) helps businesses protect their networks from such risks by ensuring that any computer connecting to the network meets corporate policy for healthy systems.

NAP is a new set of operating system components included with Windows Server 2008, Windows® XP SP3, and Windows Vista® that provide a policy-enforcement platform to help ensure that client computers on a private network meet administrator-defined requirements for system health. Checks are automatically performed for system health, such as verifying that anti-virus software is installed and current, and that the operating system is .updated as required.

NAP enforces health requirements by monitoring and assessing the health of client computers that attempt to connect or to communicate on a network. Client computers that are determined to be noncompliant with health requirements .are placed on a restricted network that contains resources for patching and updating client systems to become compliant with health policies. Administrators and technical staff can use NAP to:

* Ensure that client computers on a private network meet administrator-defined requirements for system health
* Enforce health requirements for roaming mobile computers that connect through four enforcement types, including 802.1X authenticating devices, IPsec (such as server and domain isolation), VPN Gateway, and DHCP
* Verify health status of unmanaged home computers over dial-up networking or VPN
* Verify health status of visitors' and partners' mobile computers
* Enforce policies blocking access for computers that do not meet system health, such as having no access, limited access, or deferred enforcement/unlimited access
* Enable ongoing Network and Client health monitoring

NAP also includes an application programming interface (API) set for developers and vendors to build their own components for network policy validation, ongoing compliance, and network isolation. Many vendors already participate with supporting NAP, including Cisco and TCG-TNC.

### Changes from Windows Server 2003

Windows Server 2003 supported Network Access Quarantine control, which allowed administrators to isolate VPN and Remote Access Services (RAS) users. The new Network Access Protection (NAP) features in Windows Server 2008 builds on this, adding rich, centrally managed, policy-based control, with true network isolation and system remediation capabilities. These new capabilities apply to both remote and local users.

### Benefits

Organizations can use NAP to protect their networks from viruses and other malware by ensuring that any computer connecting to the network meets corporate policy for .requirements. Network Access Protection limits network access for computers that do not meet the predefined policy, and provides remediation services to return noncompliant computers to a healthy state. It also provides ongoing compliance-checking, and remediates non-compliant computers.

## Network Policy and Access Services (NPAS) Role

Network Policy and Access Services (NPAS) in Windows Server 2008 provides technologies that let organizations deploy VPN, dial-up networking, and 802.11-protected wireless access. Administrators can define and enforce policies for network access authentication, authorization, and client health using Network Policy Server (NPS). IT staff can deploy NPS as a Remote Authentication Dial-in User Service (RADIUS) server and proxy and as a Network Access Protection (NAP) policy server.

### Changes from Windows Server 2003

Routing and Remote Access (RRAS) policies existed in previous versions of Windows Server. RRAS policies allow administrators to set which level of user is allowed to connect to the network using RRAS and VPNs. Administrators can also control settings for Secure Socket Tunneling Protocol (SSTP) and configure a quarantine. Windows Server 2008 builds on this capability and provides this type of policy based control for any computer connecting to the network.

### Benefits

Network Policy and Access Services (NPAS) replaces Routing and Remote Access (RRAS) policies. NPAS provides users with local and remote network connectivity, connects network segments, and gives network administrators a better way to centrally manage network access and client health policies. Organizations can also deploy RADIUS servers and proxy servers, and use the Connection Manager Administration Kit to create remote access profiles which allow client computers to connect to the network.

## Server Core

With Windows Server 2008, administrators can choose to install a minimal environment to help reduce administrative effort, to limit security risks, and reduce the attack surface for server roles. This type of installation is called a Server Core installation. Using Server Core also reduces time spent by administrators on server maintenance and management. Server Core installations provide a streamlined environment for running the following server roles:

* Active Directory Domain Services (AD DS)
* Active Directory Lightweight Directory Services (AD LDS)
* DHCP Server
* DNS Server
* File Services and Print Server
* Windows Media® Services
* Terminal Services (Easy Print, TS RemoteApp, and TS Gateway)
* IIS 7.0 (with some restrictions)
* Hyper-V virtualization built into Windows Server 2008

### Changes from Windows Server 2003

Server Core is a new feature in Windows Server 2008.

### Benefits

Using Server Core improves security, reduces the size of the operating system, reduces maintenance and reduces the server’s attack surface. Because a Server Core installation installs only what is required for the specified roles (DHCP Server, File Services, Print Server, DNS Server, AD LDS, or AD DS), less servicing is required than with a full installation of Windows Server 2008. Server Core installs without the full Windows Graphic User Interface and is managed remotely using Microsoft Management Console (MMC) snap-ins, or locally using command-line utilities. Server Core has a smaller disk and memory size, which increases performance, especially in virtual environments or on older hardware. The Server Core installation option is good for dedicated infrastructure, remote infrastructure, and Web servers serving static pages.

Hyper-V plus Server Core is a powerful combination. Hyper-V running on a Server Core host OS requires less patching which translates to greater uptime for the virtualization host. Server Core running as a Guest OS provides a multiplier effect benefit. Server Core is a leaner, lower-overhead system for virtual machines that perform focused infrastructure roles, allowing IT professionals to achieve greater VM density on Hyper-V servers.

## Windows Firewall with Advanced Security

Windows Firewall with Advanced Security provides the following functions on a computer that is running Windows Vista or Windows Server 2008:

* Filtering all IP version 4 (IPv4) and IP version 6 (IPv6) traffic entering or leaving the computer. By default, all incoming traffic is blocked unless it is a response to a previous outgoing request from the computer (solicited traffic), or it is specifically allowed by a rule created to allow that traffic.
* Protecting network traffic entering or exiting the computer by using the IPsec protocol to verify the integrity of the network traffic, to authenticate the identity of the sending and receiving computers or users, and to optionally encrypt traffic to provide confidentiality.

### Changes from Windows Server 2003

Beginning with Windows Vista and Windows Server 2008, configuration of both Windows Firewall and IPsec are combined into a single tool, the Windows Firewall with Advanced Security Microsoft Management Console (MMC) snap-in. The previous IPsec snap-ins are still included with Windows to manage client computers that are running Microsoft Windows Server® 2003, Windows® XP, or Windows® 2000.

In Windows Server 2003, the firewall only filtered inbound traffic.

### Benefits

Businesses need to protect their systems against security threats. The Windows Firewall with Advanced Security makes it easier to configure effective firewall and IPsec policies to protect both servers and data. The combined interface reduces the opportunities for configuring firewall rules that interfere with IPSec functionality. The more comprehensive traffic filtering features of the new Windows Firewall provide a better defense against viruses, malware, other network attacks and can help prevent threats from propagating.

## Read-Only Domain Controller (RODC)

Managing servers, services, and security at remote locations is an ongoing challenge for IT Professionals. Windows Server 2008 simplifies remote location server administration with enhancements to Active Directory, including Read-Only Domain Controllers and administrative role separation.

The Read-Only Domain Controller (RODC) is a new type of domain controller, primarily targeted toward remote locations. An RODC doesn’t store any passwords by default. That way, if the RODC is compromised, an administrator doesn’t have to worry about an intruder gaining access to the entire network using the information stored on that server. This addresses the potential lack of physical security at remote sites. RODC provides the following benefits:

* Improved security
* Faster logon times than a Windows Server 2003 full domain controller
* More efficient access to resources on the network than a Windows Server 2003 domain controller
* More securely delegate administration at remote offices

### Changes from Windows Server 2003

Before the release of Windows Server 2008, domain controller installation in a remote location presented a challenge. A read-only domain controller (RODC) is a new type of domain controller in the Windows Server® 2008 operating system that provides a way to deploy a domain controller more securely in locations that require fast and reliable authentication services but cannot ensure physical security for a writable domain controller. An RODC provides:

* With an RODC, organizations can easily deploy a domain controller for faster logon processing in locations where Active Directory was previously deployed with a Remote site configuration.
* RODCs allow local support staff to logon to the RODC to perform administrative updates just as driver updates, without having administrative access to the domain.

### Benefits

Remote locations often cannot provide the adequate physical security that is required for a writable domain controller. Furthermore, remote sites can have poor network bandwidth when they are connected to a hub site, increasing logon times and other domain functions. RODCs provide a way to improve both the security and management of remote locations.

The Remove a Domain Controller Wizard in Windows Server 2008 also increases security by providing an easy way for administrators to remove a domain controller if a system has become compromised.

## Cryptography Next Generation (CNG)

Cryptography Next Generation (CNG) is an updated cryptography tool in Windows Server 2008. Cryptography Next Generation (CNG) includes a new set of technologies, components, and APIs, providing a flexible cryptographic development platform that allows organizations to create, update, and use custom cryptography algorithms in cryptography-related applications, such as Active Directory Certificate Services (AD CS), Secure Sockets Layer (SSL), and Internet Protocol security (IPsec). CNG complies with the latest cryptographic standards and implements the U.S. government's Suite B cryptographic algorithms, which include algorithms for encryption, digital signatures, key exchange, and hashing.

### Changes from Windows Server 2003

In Windows Server 2003, cryptography was provided in CryptoAPI. CNG in Windows Server 2008 extends the functionality of CryptoAPI and makes it easier to use cryptography in software.

### Benefits

CNG gives IT staff a tool to securely perform cryptographic operations that meet Government Common Criteria requirements for storing keys. IT staff can use CNG to:

* Install and use additional cryptographic providers
* Perform basic cryptographic operations, such as creating hashes and encrypting and decrypting data
* Create, store, and retrieve cryptographic keys

## Windows BitLocker Drive Encryption

Information loss can be very costly. As more businesses and services are moving into an online mode, data has become more vulnerable. At the same time, there is a growing need among consumers that this data be protected. New rules and regulations at state and national levels, such as Sarbanes-Oxley (SOX) and Health Insurance Portability and Accountability Act (HIPAA), help drive the need for data protection. Windows BitLocker Drive Encryption (BitLocker), an integral new security feature in Windows Server 2008, protects servers at remote locations. BitLocker provides enterprise solutions to protect sensitive data for a variety of applications. BitLocker is a security feature in the Windows Vista and Windows Server 2008 operating systems that can provide protection for the operating system on computers and the data stored on the operating system volume. BitLocker performs two functions. It:

* Encrypts all data stored on the Windows operating system volume (and configured data volumes). This includes the Windows operating system, hibernation and paging files, applications, and data used by applications
* Is configured by default to use a Trusted Platform Module (TPM) to help ensure the integrity of early startup components (components used in the earlier stages of the startup process), and "locks" any BitLocker-protected volumes so that they remain protected even if the computer is tampered with when the operating system is offline

### Changes from Windows Server 2003

Windows BitLocker Drive Encryption is a new feature in Windows Server 2008 and can be used in conjunction with the Encrypting File System (EFS) to encrypt all operating system and user data on a server.

### Benefits

Windows BitLocker Drive Encryption helps to protect data on lost, stolen, or inappropriately decommissioned computers by encrypting the entire volume and checking the integrity of early boot components. Data is decrypted only if those components are successfully verified and the encrypted drive is located in the original computer. Integrity checking requires a compatible Trusted Platform Module (TPM).

## Encrypting File System (EFS)

Encrypting File System (EFS) provides the core file encryption technology used to store encrypted files on NTFS file system volumes. Users do not have to manually decrypt an encrypted file before using it; they can open and change the file as usual.

### Changes from Windows Server 2003

Enhancements to EFS include the ability to store encryption certificates on smart cards, per-user encryption of files in the client-side cache, additional Group Policy options, and a new rekeying wizard.

### Benefits

EFS is enhanced to improve performance by avoiding unnecessary re-encryption of files that have been opened but not changed.

## Federated Rights Management & Active Directory Rights Management Services

Windows Server 2008 enables a new way to protect sensitive information that is both more comprehensive and easier to administer. As in Windows Server 2003, Active Directory Federation Services (AD FS) enables one organization to set up a federated trust with another organization. Users sign on once—to their local domain—and gain access to a partner domain through identity and access federation.

### Changes from Windows Server 2003

Because Active Directory Rights Management Services (AD RMS) has been integrated with AD FS in Windows Server 2008, a federated trust now allows AD RMS to grant appropriate RMS permissions to an external user without requiring him or her to sign in locally, or to have his or her own AD RMS server. For Windows Server 2008, Active Directory Rights Management Services (AD RMS) includes several new features that were not available in Microsoft Windows Rights Management Services (RMS). These new features were designed to ease administrative overhead of AD RMS and to extend its use outside of your organization. These new features include:

* Inclusion of AD RMS in Windows Server 2008 as a server role
* Administration through a Microsoft Management Console (MMC)
* Integration with Active Directory Federation Services (AD FS)
* Self-enrollment of AD RMS servers
* Ability to delegate responsibility by means of new AD RMS administrative roles

### Benefits

With Windows Server 2008 and RMS, organizations have the needed collaboration platform and tools to enable colleagues and trusted partners to share information and work together effectively across organizational boundaries. Organizations can also better leverage their investment in Microsoft Office since RMS features are built-into Microsoft productivity products.

# Virtualization

Organizations that want to reduce costs and simplify system management are increasingly using or evaluating virtualization for server consolidation and other cost-saving technology. Microsoft Virtual Server 2005 R2 Service Pack 1 (SP1), the current server offering, remains a leader in compatibility and industry support. To meet the expanded need for virtualization, Microsoft developed Hyper-V, a next-generation, 64-bit virtualization technology that reduces costs, increases hardware utilization, optimizes network and business infrastructure, and improves server availability.

## Terminal Services (TS) Presentation Virtualization

In addition, virtualization is also enhanced in Windows Server 2008 via Terminal Services (TS) presentation virtualization. TS presentation virtualization, which separates where the application is used from where it is run, accelerates application deployments and enables any client to run any application. TS instantly web-enables rich applications to efficiently connect remote workers from managed or unmanaged devices and low or high bandwidth networks. TS helps keep critical intellectual property secure and radically simplifies regulatory compliance by removing applications and data from the desktop. For more information on Terminal Services, see the and sections of this document.

## Virtualization through Hyper-V

Hyper-V is part of Windows Server 2008 and is managed using familiar Windows-based server management tools. Hyper-V is part of the Microsoft datacenter-to-desktop virtualization strategy that delivers the benefits of virtualization at all levels of a company’s IT infrastructure. Its server virtualization features can benefit large organizations with hundreds of servers or small remote sites with just a few servers. Hyper-V provides the following benefits:

* Enables Virtual Machines to take advantage of very large amounts of memory, powerful multi-core processors, dynamic storage solutions, and the latest generation of fast networking functionality.
* Allows organizations and offices of any size from remote offices to Datacenters to benefit from virtualization features in Windows Server 2008 as part of Hyper-V, such as centralized management and monitoring, automated backup, and industry-standard management tools. This enables remote locations to operate without local IT staffs, with the remote site servers being completely managed and backed up by the central office.
* Virtual Machines can leverage powerful clustering, backup, and security features to keep the network running as smoothly as possible through demand spikes, increased workload, or server problems.
* Hyper-V’s quick migration feature enables VMs to be moved to other servers, automatically or manually, with minimal downtime.

### Changes from Windows Server 2003

Hyper-V expands on the virtualization capabilities available in Microsoft Virtual Server 2005 R2 by offering important features, such as 64-bit guest operating system support, quick migration, and greater scalability. Hyper-V requires the Windows Server 2008 x64 Edition.

### Benefits

Organizations don’t have to purchase additional software to take advantage of powerful virtualization features like 64-bit guest operating system support and quick migration. For customers who want a complete server management solution that works with VMs and physical servers, the Microsoft System Center product line now includes advanced Virtual Machine management and monitoring. Hyper-V’s open architecture enables internal development teams and third-party software developers to build enhancements to the technology and tools of third-party products. Management of the virtual environment is fully integrated with Microsoft’s management tools. This provides rapid adoption and ease of training due to the familiarity of tools already in place in the physical environment.

# Providing Remote Access

In today’s business world where employees are frequently are out of the office and access network servers remotely, organizations need a better way to control and manage remote access to systems. Terminal Services in Windows Server 2008 provide IT staff with a variety of ways to provide remote Web and application access, increase security and better manage remote access in their networks.

## Terminal Services Role

The Terminal Services server role in Windows Server 2008 provides technologies that enable users to access Windows-based programs that are installed on a terminal server, or to access the full Windows desktop. With Terminal Services, users can access a terminal server from within a corporate network or from the Internet. Terminal Services reduces the need for Virtual Private network infrastructure by supporting HTTPS access to published desktops and applications.

### Changes from Windows Server 2003

Terminal Services roles that have either been enhanced or are new in Windows Server 2008 include: Terminal Services core functionality, TS RemoteApp, TS Web Access, TS Gateway, TS Licensing, TS Session broker, and Terminal Service Windows and Resource Manager.

### Benefits

Terminal Services enhancements in Window Server 2008 enables organizations to set up a centralized system that allows them to quickly and securely provide access to Windows-based applications from any network-connected location. Customers can provide this functionality using a variety of clients, including Windows-based PCs, Windows-based thin clients or Windows Mobile®-based devices.

## Terminal Service Core Functionality

Windows Server 2008 Terminal Services includes these new core functionality features that enhance the end-user experience when connecting remotely to a Windows Server 2008 terminal server: Remote Desktop Connection 6.0, Plug and Play device redirection, Microsoft Point of Service for .NET Framework redirection, and remote desktop connection display improvements.

* Remote Desktop Connection 6.0 software is available for use on Microsoft Windows Server 2003 with Service Pack 1 (SP1) and Windows XP with Service Pack 2 (SP2). To take advantage of the new Terminal Services core functionality, organizations will need to use Remote Desktop Connection 6.0 and Windows Server 2008 configured as a terminal server.
* Redirection is enhanced and expanded in Windows Server 2008. Now you can redirect Windows Portable Devices, specifically media players based on the Media Transfer Protocol (MTP), and digital cameras based on the Picture Transfer Protocol (PTP).
* In Windows Server 2008, you can redirect devices that use Microsoft Point of Service (POS) for .NET 1.11. Microsoft POS for .NET device redirection is only supported if the terminal server is running an x86-based version of Windows Server 2008.
* Remote desktop connection functionality is improved in Windows Server 2008. The Remote Desktop Connection 6.0 software adds support for using higher-resolution desktop computers and for spanning multiple monitors horizontally to form a single, large desktop. Also, the Desktop Experience feature and the display data prioritization settings are designed to enhance the end-user experience when connecting remotely to a Windows Server 2008 terminal server.

### Changes from Windows Server 2003

Enhancements to Terminal Server core functionality include remote desktop connection, plug and play device redirection, .NET redirection, and remote desktop displays. These features automatically detect hardware, ensure that display, keyboard and mouse data passed over a remote connection is not adversely affected by bandwidth-intensive action, and enhance the end-user experience.

### Benefits

Terminal Services includes new core functionality that enhances the end-user experience when connecting remotely to a Server 2008 terminal server. Terminal Services provides technologies that enable access, from almost any computing device, to a server running Windows-based programs or the full Windows desktop.

## TS RemoteApp

End users running applications remotely often encountered slow access speed or issues in the way that the application displays or works on their computer. With the previous version of Windows Server, users had to open the desktop of the remote host, and then switch between the remote desktop and their local desktop. Using Windows Server 2008, when users launch the remote application, it looks and feels like other applications running locally on the client computer.

Microsoft has addressed remote access issues with TS RemoteApp, which is built in to Terminal Services in Windows Server 2008. RemoteApps are programs that are accessed remotely using Terminal Services, and they appear as if they are running locally, on the end user’s computer. Users can run RemoteApps side by side with their local programs. A user can minimize, maximize, and resize the program window, and can easily start multiple programs at the same time. If a user is running more than one RemoteApp on the same terminal server, the RemoteApps will share the same Terminal Services session.

### Changes from Windows Server 2003

TS RemoteApp is a new feature built into Windows Server 2008. For a program to run as a RemoteApp, the terminal server that hosts the program must be running Windows Server 2008. Any program that can run in a Terminal Services session or in a Remote Desktop session should be able to run as a RemoteApp. With previous versions of Windows Server, users had to open the desktop of the remote host, and then switch between the remote desktop and their local desktop.

### Benefits

TS RemoteApp enables organizations to provide access to standard Windows-based programs from virtually any location and lets users can run programs from a remote location side-by-side with their local programs. TS RemoteApp extends the power of Windows software to almost any client platform. It provides a user experience that is indistinguishable from running an application locally, meaning the user doesn’t need to manage two (or more) desktop environments on a single monitor.

## TS Web Access

Terminal Services Web Access (TS Web Access) is a role service in the Terminal Services role that allows IT Professionals to publish Terminal Services RemoteApp (TS RemoteApp) programs to users in an easy to access Web browser. TS Web Access provides a solution that works with minimal configuration. The TS Web Access Web page includes a customizable Web Part, which can be incorporated into a customized Web page or a Microsoft Windows SharePoint Services site.

### Changes from Windows Server 2003

TS Web Access is a new feature built into Windows Server 2008.

### Benefits

By using TS Web Access, there is less work for the administrator. IT staff can easily deploy programs from a central location. Because programs are running on a terminal server and not on the client computer, they are easier to maintain. For end users, it provides a centrally-located Web page, which makes remote applications easy to access and launch. Many organizations may be able to replace VPN solutions with HTTPS access to TS Web Access.

## Terminal Services Gateway

Controlling and managing user’s remote access to network servers is often a time-consuming process for IT staff. Terminal Services Gateway (TS Gateway) is a new server role that enables remote access to servers and workstations on the internal network with firewalls and network address translators. TS Gateway allows authorized remote users to use the Internet to log on to terminal servers on a corporate network from any location. IT staff and administrators can use these TS Gateway features:

* IT Professionals can use the TS Gateway Manager snap-in console to configure authorization policies that define conditions which remote users must meet to connect to internal network resources—for example, which user groups can connect to internal resources, what resources that they can access, and whether disk and device redirection is allowed. It can also be used to monitor TS Gateway connection status, health, and events.
* IT staff can configure TS Gateway servers and Terminal Services clients to use Network Access Protection (NAP) or use TS Gateway server with Microsoft Internet Security and Acceleration (ISA) Server to further enhance security.

### Changes from Windows Server 2003

TS Gateway transmits RDP traffic over port 443, the standard HTTP Secure Sockets Layer/Transport Layer Security (SSL/TLS) tunnel port. Because most corporations open port 443 to enable Internet connectivity, TS Gateway takes advantage of this network design to provide remote access connectivity across multiple firewalls, allowing access to computers on the internal network without requiring a VPN connection.

### Benefits

With TS Gateway, users can connect to their corporate network from remote places, such as hotels or client sites, by means of the Internet without having to use a VPN to secure access to the corporate network. This enhances corporate security while also simplifying the user experience for accessing remote applications. Remote Desktop connections are available in Windows Server 2003, Windows XP, Windows Vista, and Windows Server 2008. TS Gateway improves the end-user experience when remotely running applications, and makes it easier to IT staff to set up network authorization policies, configure systems, and monitor the health of the server network. TS Gateway may allow organizations to replace VPN infrastructures with HTTPS access.

## Terminal Services Licensing

It is often difficult and time-consuming to track licenses for devices that connect to terminal servers. Microsoft has simplified this process with enhancements to the licensing process, which makes it easier to set up and maintain licenses. Windows Server 2008 provides a license management system known as Terminal Services Licensing (TS Licensing). This system allows terminal servers to obtain and manage Terminal Services client access licenses (TS CALs) for devices and users that are connecting to a terminal server.

### Changes from Windows Server 2003

TS Licensing for Windows Server 2008 now includes the ability to track the issuance of TS per User CALs by using TS Licensing Manager.

### Benefits

TS Licensing manages unlicensed, temporarily licensed, and client-access licensed clients, and supports terminal servers that run Windows Server 2008 as well as the Microsoft Windows Server 2003 operating systems. TS Licensing works with TS itself to provide, catalog, and enforce license policy among Terminal Server clients. Using TS Licensing makes license management easier for system administrators and helps prevent organizations from under- or-over-purchasing licenses. TS Licensing is used only with Terminal Services and not with Remote Desktop. TS Licensing includes the following features and benefits:

* Centralized administration for TS CALs and their corresponding tokens
* License tracking and reporting for per-user licensing mode
* Support for various communication channels and purchase programs
* Minimal impact on network and servers

## TS Session Broker

The Terminal Services Session Broker (TS Session Broker) role service in Windows Server 2008 allows a user to reconnect to an existing session in a load-balanced terminal server farm. This feature enables IT staff to distribute the session load between servers in a load-balanced terminal server farm. This solution is recommended for terminal server farms of two to five servers. TS Session Broker stores session state information that includes session IDs and their associated user names, and the name of the server where each session resides.

### Changes from Windows Server 2003

Windows Server 2008 introduces a new TS Session Broker feature—TS Session Broker load balancing. This feature allows businesses to distribute the session load between servers in a load-balanced terminal server farm. This solution is easier to deploy than Windows Network Load Balancing (NLB), and is recommended for terminal server farms of two to five servers. In Windows Server 2008, the name of the Terminal Services Session Directory (TS Session Directory) feature is changed to Terminal Services Session Broker (TS Session Broker).

### Benefits

TS Session Broker makes it easier for IT staff to reconnect to sessions and redistribute the session load between servers in a load-balanced terminal server farm. This will save the organization time and reduce potential problems with server response and performance.

# Active Directory Enhancements

Windows Server 2008 contains many new or enhanced Active Directory features that let IT Professionals boost their productivity, optimize their infrastructure, and ensure unprecedented protection.

## Active Directory Domain Services Role

Active Directory Domain Services (AD DS) in Windows Server 2008 stores information about users, computers, and other devices on the network. It also manages computers and users roles through a set of policies. Enhancements to Windows Server 2008 include:

* You can now set up Active Directory Domain Services (AD DS) auditing to log changes to AD DS objects and their attributes. The log lists the setting of the changed object as it was before the change and the setting it was changed to. This provides IT staff with a method to track changes and improve security.
* The Windows Server 2008 operating system provides organizations with a way to define different password and account lockout policies for different users or groups of users in a domain. Password policies can be assigned to individual user accounts or to global security groups.
* With a Read-Only Domain Controller (RODC), organizations can easily deploy a domain controller in locations where physical security cannot be guaranteed. An RODC hosts read-only partitions of the Active Directory Domain Services (AD DS) database. The RODC provides extra security that protects from attacks by limiting the chance of a stolen domain controller to be used to break into the network. An RODC only displays the passwords for accounts available on that RODC. The accounts selected by the administrator have their passwords cached on the RODC. If the system is attacked, the intruder would have access to fewer passwords.
* Administrators can stop and restart Active Directory Domain Services (AD DS) in Windows Server 2008 by using Microsoft Management Console (MMC) snap-ins or the command line. Restartable AD DS reduces the time that is required to perform certain operations. AD DS can be stopped so that updates can be applied to a domain controller. Administrators can stop AD DS to perform tasks such as offline defragmentation of the Active Directory database or upgrade Active Directory, without restarting the domain controller.
* The data mining tool (Dsamain.exe) can improve recovery processes for organizations by providing a means to compare data as it exists in snapshots or backups that are taken at different times so that you can better decide which data to restore after a data loss. Data mining can provide information on OU or objects that were deleted.

### Changes from Windows Server 2003

New or updated Active Directory Domain Services include AD DS Auditing, Password Policies, Read-Only Domain Controllers, Restartable Active Directory Domain Services, and Snapshot Exposure.

### Benefits

Enhancements in AD DS help administrators increase security with AD DS Auditing, AD DS Fine-Grained Password Policies, and RODC. A restartable AD DS will save both time and money, as well as lower downtime, because it reduces the time that is required to perform certain operations, such as updating a domain controller or offline defragmentation of the Active Directory database, without restarting the physical server. The data mining tool (Dsamain.exe) can be used to obtain information on data contained in snapshots or backups.

## Active Directory Certificates Services Role

The Active Directory Certificates Services Role (AD CS) includes features that let administrators manage certificate enrollment and revocation in a variety of scalable environments. Organizations can use AD CS to track and generate PKI certificates online, set up and maintain PKI group policies, as well as track the status of certificates. Another new AD CS feature, the Network Device Enrollment Service (NDES), is a communication protocol that makes it possible for software running on network devices, such as routers and switches that cannot otherwise be authenticated on the network, to enroll for X.509 certificates from a certification authority (CA). Specific enhancements in AD CS include:

* Microsoft Online Responder, which is based on and compliant with RFC 2560 for Online Certificate Status Protocol (OCSP). Online Responder can be used to simplify management and distribute revocation status information for public key infrastructures (PKIs). Unlike Certificate Revocation Lists (CRLs), an Online Responder receives and responds only to requests from clients for information about the status of a single certificate.
* Certificate-related Group Policy, which lets administrators manage certificate validation settings according to the security needs of the organization.
* The Network Device Enrollment Service (NDES) is the Microsoft implementation of the Simple Certificate Enrollment Protocol (SCEP), a communication protocol that makes it possible for software running on network devices such as routers and switches, which cannot otherwise be authenticated on the network, to enroll for X.509 certificates from a certification authority (CA).
* A new enrollment control helps IT staff more easily implement Web enrollment. The Web enrollment support allows users to request and obtain new and renewed certificates over an Internet or intranet connection.
* Enterprise PKI, a Microsoft Management Console (MMC) snap-in for Windows Server 2008 that can be used to analyze the health state of CAs installed on computers running Windows Server 2008 or Windows Server 2003. PKIView, now an MMC snap-in for Windows Server 2008, provides a view of the status of a network’s PKI environment.

### Changes from Windows Server 2003

There are a number of changes in Windows Server 2008, including:

* Enterprise PKI, a Microsoft Management Console (MMC) snap-in for Windows Server 2008 used to analyze PKI health. Previously called the PKI Health tool, this was originally part of the Microsoft Windows Server 2003 Resource Kit.
* Several Group Policy settings are also added to enhance the management of OCSP and CRL data use.
* The previous enrollment control, XEnroll.dll, is replaced in Windows Vista and Windows Server 2008 with a new enrollment control, CertEnroll.dll. The new CertEnroll.dll is designed to be more secure, easier to script, and easier to update than XEnroll.dll was.

### Benefits

Fundamental changes to Active Directory Certificate Services in Windows Server 2008 can help organizations improve security, manageability, and interoperability.

## Active Directory Federation Services Role

Active Directory Federation Services (AD FS) provides Web Single Sign-On (SSO) technologies to authenticate a user to multiple Web applications over the life of a single online session. This authentication allows organizations to trust user accounts from partner organizations. Active Directory Federation Services (AD FS) is a server role in Microsoft Windows Server 2008 that is part of a larger identity access and management solution.

Active Directory Federation Services in Windows Server 2008 includes improvements to the installation experience, configuration wizard, and enhancements that increase its ability to integrate with other applications, such as Microsoft Office SharePoint® Services 2007 and Active Directory Rights Management Services.

### Changes from Windows Server 2003

Active Directory Federation Services is included in Windows Server 2008 as a server role, and there are new server validation checks in the installation wizard. AD FS is more tightly integrated with Office SharePoint Server 2007 and Active Directory Rights Management Services (AD RMS.)

### Benefits

For Windows Server 2008, AD FS includes new functionality that was not available in Windows Server 2003 R2. This new functionality is designed to ease administrative overhead and to further extend support for key applications. It includes the following benefits:

* A better administrative experience when you establish federated trusts—improved trust policy import and export functionality helps to minimize partner-based configuration issues that are commonly associated with federated trust establishment
* Improved installation through new server validation checks in the installation wizard
* Improved application support between SharePoint Server 2007 and Active Directory Rights Management Services (AD RMS)

## Active Directory Lightweight Directory Services Role

Active Directory Lightweight Directory Service roles (AD LDS) in Windows Server 2008 provide flexible support for directory-enabled applications. With AD LDS, organizations can run multiple instances of AD LDS concurrently on a single computer, with an independently managed schema for each AD LDS instance or configuration set (if the instance is part of a configuration set). AD LDS provides data storage and retrieval for directory-enabled applications, without the dependencies that are required for Active Directory Domain Services (AD DS).

### Changes from Windows Server 2003

AD LDS in Windows Server 2008 replaces the functionality that Active Directory Application Mode (ADAM) provided. ADAM is available for Windows XP Professional and Windows Server 2003 operating systems. Applications that were designed to work with ADAM do not require changes to function with AD LDS.

### Benefits

Organizations that have applications which require a directory for storing application data can use AD LDS as the data store. With this functionality, organizations could use AD LDS during application testing, or deploy it in support of a directory enabled application. Any application that requires Schema changes in AD can be directed to use AD LDS. This saves AD from having constant schema changes by applications and developers. In addition, AD LDS is more compatible for true X500 LDAP applications.

## Active Directory Rights Management Services Role (AD RMS)

Active Directory Rights Management Services Role (AD RMS) helps organizations create information-protection solutions. It will work with any AD RMS-enabled application to provide persistent usage policies for sensitive information. Content that can be protected by using AD RMS includes intranet Web sites, e-mail messages, and documents. AD RMS includes a set of core functions that allow developers to add information protection to the functionality of existing applications.

### Changes from Windows Server 2003

In the earlier versions of RMS, administration was done through a Web interface. In AD RMS, the administrative interface has been migrated to an MMC snap-in console. AD RMS console gives you all the functionality available with the earlier version of RMS but in an interface that integrates with AD FS.

### Benefits

AD RMS in Windows Server 2008 brings many improvements to both the installation and administration experience. New features were designed to ease administrative overhead in AD RMS and to extend its use outside of your organization. These new features include:

* Integration with Active Directory Federation Services (AD FS), enabling RMS protection to documents across organizations
* Administration through a Microsoft Management Console (MMC)
* Inclusion of AD RMS in Windows Server 2008 as a server role
* Self-enrollment of AD RMS servers
* Ability to delegate responsibility by means of new AD RMS administrative roles

# Server Management Made Easier

Simplifying the day-to-day complexities of server administration is a key theme in many of the enhancements included in Windows Server 2008. New management tools like the Server Manager Console provide a single, unified console for managing a server's configuration and system information, displaying server status, identifying problems with server role configuration, and managing all roles installed on the server. Windows Server 2008 also includes powerful reliability monitoring that includes reports and logs that will provide technical staff with a concise snapshot of system performance and reliability. Windows Server 2008 helps lighten the load of Administrators with powerful scripting for every administration task.

## Server Manager

Server Manager provides a single source for managing a server's identity and system information, displaying server status, identifying problems with server role configuration, and managing all of the roles installed on the server. Administrators no longer have to run the Security Configuration Wizard before deploying servers: With Server Manager, server roles are configured with recommended security settings by default, and are ready to deploy as soon as they are installed and properly configured. Server Manager makes server administration more efficient by allowing administrators to use a single tool to do the following:

* View and make changes to server roles and features installed on the server
* Perform management tasks associated with the operational life cycle of the server, such as starting or stopping services, and managing local user accounts
* Perform management tasks associated with the operational life cycle of roles installed on the server
* Determine server status, identify critical events, and analyze and troubleshoot configuration issues or failures
* Install or remove roles, role services and features by using a Windows command line

### Changes from Windows Server 2003

Windows Server 2003 contained features that helped organizations manage their systems. In Windows Server 2008, Server Manager expands management tracking and replaces several features included with Windows Server 2003, including Manage Your Server, Configure Your Server, and Add or Remove Windows Components. Server Manager in Windows Server 2008 supports adding multiple roles and features simultaneously.

IT Professionals can also use the Windows Remote Shell (WinRS) tool to remotely manage servers or to obtain management data through Windows Remote Management (WinRM) and Windows Management Instrumentation (WMI) objects on remote servers. WinRM is a new remote access protocol that is based on the DMTF standard Web Services for Management.

### Benefits

Server Manager gives organizations and IT Professionals greater control. Role-based installation and management eases the task of managing and securing multiple server roles in an enterprise with the new Server Manager console. Configuration Wizards save time by automating many of the time consuming tasks of managing systems.

## Windows Reliability and Performance Monitor

In Windows Server 2008, Windows Reliability and Performance Monitor is a Microsoft Management Console (MMC) snap-in that provides IT Professionals with a wide range of tools to monitor and assess system performance and reliability. Windows Reliability and Performance Monitor includes:

* A graphical interface for customizing performance data collection and Event Trace Sessions
* Reliability Monitor, an MMC snap-in that tracks changes to the system and compares them to changes in system stability, providing a graphical view of their relationship
* Data Collector Set, which groups data collectors into reusable elements for use with different performance monitoring scenarios; when a group of data collectors are stored as a Data Collector Set, operations such as scheduling can be applied to the entire set through a single property change
* A wizard and template for creating and scheduling logs
* Resource View screen, which provides a real-time graphical overview of CPU, disk, network and memory usage
* A Reliability Monitor which calculates a System Stability Index that reflects whether unexpected problems reduced the reliability of the system
* Unified property configuration for all data collection, including scheduling that lets IT staff use a Data Collection Set as a template so that it does not have to be recreated
* User-friendly diagnosis reports that provide a wide variety of information and can be easily created from Data Collection Sets

### Changes from Windows Server 2003

In Windows Server 2008, Windows Reliability and Performance Monitor is a Microsoft Management Console (MMC) snap-in that combines the functionality of previous stand-alone tools, including Performance Logs and Alerts, Server Performance Advisor, and System Monitor.

### Benefits

Windows Reliability and Performance Monitor saves technical staff time by making it easier to locate information about the status and performance of servers. Powerful scripts let administrators customize and save Data Collection Sets as templates so that they can be reused.

# Web Hosting

Windows Server 2008 delivers a unified platform for Web publishing that integrates Internet Information Services (IIS), ASP.NET, and Windows Communication Foundation (WCF). IIS version 7.0 is a major enhancement to the existing IIS Web server and plays a central role in integrating Web platform technologies.

## Internet Information Services (IIS)

In Windows Server 2008, IIS 7.0 contains a number of features that let organizations simplify Web server management with advanced and easy-to-use options. IIS 7.0 provides many new features relating to the Web:

* It offers a broad set of management features that simplify the day-to-day tasks of managing Web sites and applications.
* IIS 7.0 enables those who host or administer Web sites or WCF services to delegate administrative control to developers or content owners, to reduce cost of ownership and administrative burden for server administrators.
* IIS 7.0 is made up of more than 40 separate feature modules. Organizations can choose which features to install and run on their Web server. The ability to run only the modules required for the environment can reduce administrative overhead.
* It provides a clear view of internal diagnostic information about IIS, and collects and surfaces detailed diagnostic events to aid troubleshooting problematic servers.
* IIS 7.0 allows storing IIS configuration settings in web.config files, which makes it much easier to use Xcopy to deploy applications across multiple front-end Web servers to reduce costly and error-prone replication and manual synchronization issues.
* IIS 7.0 extensibility includes an all-new core server application programming interface (API), as well as configuration, scripting, event logging, and administration tool feature-sets, which provides organizations with a complete server platform on which to build Web server extensions.
* Microsoft Windows Media® Services 9 Series is an industrial-strength platform for streaming live and on-demand digital media content. IT staff can add a Streaming Media Services role to the Server Core installation option of the Windows Server 2008 operating system to use the streaming media server features.

### Changes from Windows 2003

IIS 7.0 is built to be compatible with existing releases. All existing ASP, ASP.NET 1.1, and ASP.NET 2.0 applications will run on IIS 7.0 without any code changes (using the compatible ISAPI support). Some features or ways of implementing tasks have changed in the new version. IIS 7.0:

* Introduces some major improvements to the way configuration data is stored and accessed. These changes make administering the server and supporting Web applications easier.
* Is built to be compatible with existing ASP, ASP.NET 1.1, and ASP.Net 2.0 applications while extending management, performance, and troubleshooting capabilities. IIS 7.0 changes the way configuration data is stored, the way code is processed, and can be configured in a completely modular fashion.
* Allows users to configure Windows NT® token-based Web Agent settings with the IIS Manager snap-in.

### Benefits

IIS 7.0 offers a broad set of management features that simplify the day-to-day tasks of managing Web sites and applications. The new IIS Manager reduces administrative workload and saves time. It also allows administrators to delegate administrative control over individual Web sites to the developers or content owners, reducing the workload for the IT staff. The troubleshooting features of IIS 7.0 help administrators and developers isolate problems more easily. The modular design allows administrators to configure their Web servers with only the functionality required in the environment. This can enhance performance and reduce the attack surface.

# Automating Tasks

IT Professionals often spend too much time performing mundane maintenance tasks on systems rather than using their skills to address critical business needs. Microsoft has added a powerful new scripting environment to Windows Server 2008, called Windows PowerShell. This will help IT staff automate some of the most frequently performed maintenance tasks.

## Windows PowerShell

Windows PowerShell is a new command-line shell and task-based scripting technology that provides comprehensive control and automation of system administration tasks, with the goal of increasing IT productivity. Windows PowerShell includes numerous system administration utilities, consistent syntax and naming conventions, and improved navigation of common management data such as the registry, certificate store, or WMI. Windows PowerShell also includes an intuitive scripting language specifically designed for IT administration. Windows PowerShell includes 130 scripts and will also work with existing scripts.

### Changes from Windows 2003

Windows PowerShell is a new feature that was not available in Windows Server 2003.

### Benefits

Windows PowerShell is designed to accelerate the automation of system administration. It provides a new administrator-focused scripting language and more than 130 standard command-line scripts to enable easier system administration and accelerated automation. Larger enterprises can automate management of multiple servers using Windows PowerShell. Among other benefits, Windows PowerShell provides:

* Improved productivity by allowing IT organizations to automate tasks that are manual and time-consuming
* Accelerated automation of system administration
* Expanded scripts that are easy to use and work with existing scripts
* Access to an active PowerScript developer community that produces Cmdlets to automate complex tasks

# Application Enhancements

In Windows Server 2008, the Application Server Role and Application Server Foundation–Windows Communication Foundation (WCF), .NET Framework, Windows Workflow Foundation (WF), Windows Activation Service (WAS), and Windows Presentation Foundation (WPF)–help control how applications function. It is a world-class application server, supporting rich Web and server-based applications and providing a strong collaboration platform out of the box. Workgroups use the Windows SharePoint Services role to manage documents.

## Windows Activation Service (WAS)

To enhance the development and hosting of WCF services over many protocols, Windows Server 2008 includes Windows Activation Service (WAS.) WAS provides all types of message-activated applications with intelligent resource management, on-demand process activation, health-monitoring, and automatic failure detection and recycling.

## Application Server Role and Application Server Foundation

Application Server is a new server role in Windows Server 2008. Application Server provides an integrated environment for deploying and running custom, server-based business applications. These applications respond to requests that arrive over the network from remote client computers or from other applications. Application Server provides the following:

* A runtime that supports effective deployment and management of high-performance server-based business applications.
* The .NET Framework 3.0., which gives developers a simplified programming model for connected server applications. The Application Server Foundation is the group of technologies that are installed by default when you install the Application Server role. Essentially, Application Server Foundation is the .NET Framework 3.0.
* A new user-friendly Add Roles Wizard that helps IT staff choose the role services and features necessary to run applications.

# Better Together with Windows Vista

Deploying Windows Vista® SP1 and Windows Server® 2008 concurrently is more efficient for IT Professionals, leveraging common deployment processes and tools. The common code base makes possible a more integrated management and security infrastructure, and facilitates advances in network performance and computing-model flexibility. The following are benefits of deploying both Windows Server 2008 and Windows Vista:

* Network Access Protection (NAP) features in Windows Server 2008 help ensure that Windows Vista clients connecting to the network are compliant with security policies, and if not, are then restricted from accessing network resources.
* Windows Deployment Services (WDS), an update of Remote Installation Service (RIS), provides a simplified, secure means of rapidly deploying Windows operating systems to PCs and Servers by using network-based installation, without the need for an administrator to work directly on each computer, or to install Windows components from CD or DVD media. Two forms of multicasting—ScheduledCast and AutoCast—allow both scheduled ‘push’ and client ‘pull’ deployments while conserving bandwidth.
* Windows Server 2008 includes features of Windows Vista, such as Windows Media Player and desktop themes. To maximize server performance in default configurations, the Desktop Experience feature does not enable any of the Windows Vista features by default; IT staff must do so manually.
* Server resources are cached locally, so that they are available even if the server is not, and copies update automatically when the client and server are reconnected. Synchronization uses differential copy to further reduce network bandwidth use.
* Concurrent deployment enables more integrated system architecture and delivers system-wide performance improvements, including network file sharing, audio/video/data communication QoS and faster search.
* Server Message Block (SMB) 2.0 technology, incorporated into both Windows Vista and Windows Server 2008, improves file-sharing performance over high-latency links by compounding operations and reducing the number of ‘round trips’ and increasing buffer sizes.
* Both Windows Vista and Windows Server 2008 provide fast file searching to enable streamlined client access to files. Indexing of Division/Departmental servers running Windows Server 2008 accelerates search across desktop and network resources.
* Windows Server 2008 and Windows Vista use a new file-based image format (WIM), simplifying image management and reducing the number of images deployed.
* New technologies like SMB 2.0, TCP Receive Window Auto-Tuning, and Compound TCP (CTCP) provide faster communications when Windows Vista clients are downloading files from Windows Server 2008 file shares.

### Changes from Windows Server 2003

Both the Windows Server 2008 operating system and the Windows Vista operating system provide many new and enhanced features and business benefits on their own. However, when both operating systems are installed, organizations can realize additional benefits, including more efficient management, greater availability, and faster communications. Features or enhancement in Windows Vista and Windows Server 2008 include: additional features in DNS client software, the new Network Access Protection, updates to the Windows Deployment Services, changes in Terminal Services, changes in policies, enhanced indexing and search, as well as changes in client print management. Windows Security Health Agent and Windows Security Health Validator are included with the Windows Server 2008 and Windows Vista operating systems.

### Benefits

Deploying Windows Vista® SP1 and Windows Server® 2008 concurrently is more efficient for IT Professionals leveraging common deployment processes and tools. Windows Deployment Services (WDS) enables automated deployment of file-based images for both servers and client PCs, and Volume Activation 2.0 provides a more efficient process for managing licenses. Once deployed, advanced management and security capabilities are enabled, including Network Access Protection (NAP) to quarantine remote PCs until compliance can be ensured; expanded Group Policy covering both client PCs and the network environment; and network protocols to optimize bandwidth use and improve file sharing.

# Remote Sites

Remote sites have historically been an IT headache. Often, there is no local IT staff, and it can be both expensive and difficult to deploy software and security updates there. It is often difficult to enforce security and IP standards in a remote site. Windows Server 2008 includes many features that help an organization’s IT staff manage remote locations more easily and securely. These features include:

* Hyper-V: With the Hyper-V virtualization built into Windows Server 2008, remote office servers with multiple functions—such as print services, fax services, and remote access—can be designed, assembled, and tested at the central office, and then shipped to the remote site on a DVD or on a preconfigured computer, saving installation time and costs.
* [Read-Only Domain Controller (RODC)](#_Read-only_Domain_Controller_(RODC)): With an RODC, organizations can easily deploy a domain controller in locations where physical security cannot be guaranteed. The RODC performs standard, inbound replication for Active Directory Domain Services (AD DS) and Distributed File System Replication (DFS-R) changes.
* BitLocker: Windows BitLocker Drive Encryption is a security feature in the Windows Vista Enterprise, Windows Vista Ultimate, and Windows Server 2008 operating systems. It is ideal for improving security in remote sites because IT staff can encrypt all of the data stored on the system volume and configured data volumes. This includes the Windows operating system, hibernation and paging files, applications, and data that applications use.
* Server Core: In Windows Server 2008, administrators can now choose to install a minimal environment using Server Core. This improves security at the remote site and makes it easier to manage remote systems.
* Network stack: Network stack improvements also make communications over high-latency links more reliable.

### Changes from Windows Server 2003

Many new features in Windows Server 2008 can be used to improve security and makes management easier at remote sites including: Server Core, Hyper-V, BitLocker, and RODC.

### Benefits

Windows Server 2008 contains many features to make remote site management and security easier for IT staff. Windows Server 2008 can:

* Improve the effectiveness of remote site server deployment and administration
* Mitigate the physical security risks in remote sites
* Improve the efficiency of WAN communications from the remote site

## Business Continuity

It is vital that organizations protect their data and maintain access to data in the event of a disaster. Windows Server 2008 can be used to support business continuity with its failover clustering, Windows Server Backup, Self-Healing NTFS, and Network Load Balancing features.

* The Windows Server Backup feature in Windows Server 2008 provides a complete solution for day-to-day backup and recovery needs. IT staff can use Windows Server Backup to protect servers efficiently and reliably, without having to consider the details of backup and recovery technology.
* Self-Healing NTFS protects file systems efficiently and reliably. Self-healing NTFS attempts to correct corruptions of the NTFS file system online, without requiring Chkdsk.exe to be run. IT professionals can use self-healing NTFS to protect the file system without having to be concerned about the details of file system technology. Much of the self-healing process is enabled by default. In the event of a major file system issue, self-healing NTFS reports problems found, along with possible solutions.
* Network Load Balancing (NLB) distributes traffic across several servers, using the TCP/IP networking protocol. In addition, NLB can be combined with Hyper-V to implement highly available server solutions.
* The transactional NTFS file system and the Transactional Registry, the kernel transactional technology in Windows Server 2008, has been enhanced to coordinate their work through transactions.

### Failover Clustering

Failover Clustering in Windows Server 2008 provides new features that an organization can use to implement a high availability strategy making cluster servers a smart business choice for the enterprise. The key value propositions include:

* The new management interface reduces complexity, which provides the user with a simple interface to create, manage and use clustered servers.
* New tools reduce upfront configuration issues, so support costs and implementation times will decrease.
* New functionality allows implementation in geographically dispersed environments, allowing the technology to adapt to the customer’s environment.

### Changes from Windows Server 2003

In Windows Server 2008, Failover Clustering (formerly known as server clusters) is enhanced. Prior to Windows Server 2008 and the addition of Self-Healing NTFS, technical staff had to use the Chkdsk.exe tool to fix corruptions of NTFS file system volumes on a disk. With Windows Server 2008, only extreme cases will require using Chkdsk.exe.

Transactions used with the file system or registry can be coordinated with any other transactional resource, such as SQL Server® or MSMQ. The command line has been extended with the Transact command to allow simple command-line scripting using transactions.

A new cluster validation wizard can be used to perform tests to determine whether a system, storage and network configuration is suitable for a cluster. The Cluster Setup wizard has been simplified so that it is easier to set up a cluster in one step. Cluster setup is also fully scriptable, so that administrators can automate cluster deployment. Using the cluster migration tool, resource group settings can be captured from a cluster running Windows Server 2003, and then applied to a cluster running Windows Server 2008.

In Windows Server 2008, administrators can configure a cluster so that the quorum resource is not a single point of failure using the hybrid quorum resource model. New functionality allows implementation in geographically dispersed environments, allowing the technology to adapt to the customer’s environment.

There are changes in Windows Server 2008 in relation to multi-site clustering. Administrators can now place clustered servers on different IP subnets, reducing the requirements for geographically dispersed clusters and the complexity of providing site resiliency for core clustered applications. The Majority Node Set (MNS) clustering is now a default; this was an SP1 hotfix add-on in Windows Server 2003.

### Benefits

Windows Server 2008 makes it easier for organizations to implement and maintain highly available server solutions. Failover clustering streamlines setup and management for clustered servers. Windows Server Backup and Self-Healing NTFS will reliably protect an organization’s data and file systems. Network Load Balancing is particularly useful for ensuring that stateless applications, such as a Web server running IIS 7.0, are scalable by adding additional servers as the load increases.

Windows Server 2008 simplifies the initial cluster deployment and its ongoing management, and improves the performance and reliability of the server. Windows Server 2008 also reduces the possibility of administrator errors when configuring and deploying clusters, and therefore improves IT efficiency. Hyper-V Host Clustering with Guest Clustering provides a tool for IT professionals to implement highly available server solutions. With reduced management requirements and better reliability, failover clusters in Windows Server 2008 are a key component in the high availability scenario needed to ensure business continuity.

# Next Generation TCP/IP Protocols and Networking Components

Windows Server 2008 networking improves performance by automatically tuning network connections to maximize throughput. It increases scalability through optimized support for multi-gigabit networks and next generation Internet protocols, to meet growing IT infrastructure demands. Windows Server 2008 networking boosts security through integrated network security features to provide a solid foundation for network workloads for today and the future. When combined with the related capabilities in Windows Vista, Windows Server 2008 offers an even more enhanced networking experience helping IT administrators provide enhanced performance, scalable and secure networking experience, helping improve user access to network resources. Windows Server 2008 and Windows Vista include many enhancements and innovations to the following protocols and networking components, which will improve network performance and reliability, increase security, and enable greater scalability for network applications:

* The Next-Generation TCP/IP stack is a significant redesign of TCP/IP functionality for both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) that meets the connectivity and performance needs of today’s varied networking environments and technologies. The Next Generation TCP/IP stack supports a dual IP layer architecture in which the IPv4 and IPv6 implementations share common transport (TCP and UDP) and framing layers.
* There are major enhancements to IPv6. Native IPv6 support across all client and server services creates a more scalable and reliable network.
* Policy-based Quality of Service (QoS) in Windows Server 2008 and Windows Vista allow IT staff to either prioritize or manage the sending rate for outgoing network traffic.
* The auto-tuning nature of the stack improves network connectivity performance in high-latency environments.
* There is extensive support for hardware-based offload and network acceleration.
* The Next Generation TCP/IP stack helps determine performance bottlenecks and network congestion.
* Windows Filtering Platform (WFP) is a new architecture in the Next Generation TCP/IP stack that provides APIs so that non-Microsoft independent software vendors (ISVs) can filter at several layers in the TCP/IP protocol stack and throughout the operating system.
* In Windows Server 2008, IPsec support for IPv6 traffic is the same as that for IPv4, including support for Internet Key Exchange (IKE) and data encryption.

### Changes from Windows Server 2003

The Windows Server 2008 TCP/IP stack represents a major redesigned. There are major enhancement to IPv6, including a new dual-IP layer architecture, and Policy-based QoS in Windows Server 2008. These changes provide enhanced connectivity, ease of use, management, reliability and security.

### Benefits

With new technologies and features like enhanced networking, Windows Server 2008 provides the most versatile and reliable Windows platform for all workload and application requirements. For example, the networking enhancements and innovations delivered in Windows Server 2008 will help enable IT Professionals to meet the increasing demands placed on their IT infrastructure, both today and well into the future. Thanks to a wide range of networking performance, scalability and security improvements in Windows Server 2008, IT Administrators will have a solid foundation on which to build their businesses. Enhancements in the TCP/IP stack, IPv6, and Policy-Based QoS give IT administrators greater and more flexible options for managing networking infrastructure, routing network traffic efficiently and effectively, and deploying protected traffic scenarios.

# Interoperability

Windows Server 2008 contains other features that improve interoperability with other operating systems, including.

* The Subsystem for UNIX-based Applications (SUA), along with a package of support utilities available for download from the Microsoft Web site, enables organizations to run UNIX-based programs, and to compile and run custom UNIX-based applications in the Windows Server 2008 environment.
* The Services for Network File System (NFS) provides a file-sharing solution for organizations that have a mixed Windows and UNIX environment. With Services for NFS, you can transfer files between computers running the Windows Server 2008 operating system and the UNIX operating system by using the NFS protocol.

### Changes from Windows Server 2003

Services for Network File System (NFS) are available for installation on 64-bit versions of Windows Server 2008 only; in other versions of Windows Server 2008, Services for NFS is available as a role service of the File Services role.

### Benefits

Windows Server 2008 provides additional features that make it easier for IT staff to do their job better. It allows IT staff to better integrate Windows and UNIX systems.

# Conclusion

Windows Server 2008 helps organizations improve service levels at a lower cost, build and operate a flexible platform to meet changing business demands, and provides capabilities to secure the IT platform. It expands the organization’s ability to control and secure network access through features like Network Access Protection (NAP), Federated Rights Management, Read-Only Domain Controller (RODC), Cryptography Next Generation (CNG), Rights Management System, Windows Firewall with Advanced Security, and Encrypting File System (EFS).

The Hyper-V virtualization technology in Server 2008 provides the ability to move disparate servers to Virtual Machines (VMs) in a centrally-managed environment. Windows Server 2008 extends Web capabilities to help organizations deliver rich Web-based experiences efficiently and effectively, with improved administration and diagnostics, development and application tools, and lower infrastructure costs.

Windows Server 2008 provides a versatile and reliable Windows platform designed to meet an organization’s workload and application requirements. It helps administrators with powerful scripting, administration, configuration, and deployment features in Server Manager, Windows PowerShell, and Windows Deployment Services. Windows Server 2008 includes many features that help an organization’s IT staff manage remote locations more easily and securely. Features in Hyper-V, Read-only Domain Controller, and BitLocker help organizations provide enterprise-class networking, security, and virtualization to remote sites.

# Comparison of Features in Windows Server 2003 and Windows Server 2008

Table 1: Features in Windows Server 2003 R2 versus Windows Server 2008

The following table lists all of the features contained in Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 Server Core. Information is also provided for which edition contains the feature. Symbols indicate whether the feature is included, partially included, or not included.

|  |  |  |  |
| --- | --- | --- | --- |
| **Key**: | Feature included or supported =Feature included  | Feature partially supported = Feature partially supported  | Feature not included = Not Included |

| **Feature** | Windows Server 2003 Web R2 | Windows Server 2003 Standard R2 | Windows Server 2003 Enterprise R2 | Windows Server 2003 Data Center R2 | Windows Server 2008 Web | Windows Server 2008 Standard | Windows Server 2008 Enterprise | Windows Server 2008 Data Center | Windows Server 2008Server Core |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Server Role** |
| Active Directory® Certificate Services (AD CS) | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| Administrator Role Separation–Active Directory Domain Services (AD DS) | Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Read Only Domain Controller – Active Directory Domain Services (AD DS)  | Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Restartable Active Directory – Active Directory Domain Services | Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Active Directory Federation Services | Feature not included | Feature not included | Feature partially supported | Feature partially supported | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature not included |
| Claims Aware Application Agent | .Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature not included |
| Active Directory Lightweight Directory Services (AD LDS) | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Federated Rights Management – Active Directory Rights Management Services (AD RMS) | Feature not included | Feature not included | Feature partially supported | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature not included |
| **Application Server** |
| DHCP Server | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| DHCP Server – Clustered DHCP Server | Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| DNS Server | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Fax Server | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| File Server | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| File Server-Windows Search Service | Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| File Server-Services for Network File System | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| Network Access Services-Network Policy Server | Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| Network Access Services-Remote Access Service | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| Network Access Services-Health Registration Authority | Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| Network Access Services-Connection Manager Administration Kit | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| Network Access Services-System Health Validator Templates | Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| Print Server | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Print Server-Import and Export Print Settings | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Print Management Console |  Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Terminal Services | Feature partially supported | Feature partially supported | Feature included or supported | Feature included or supported | Feature not included | Feature partially supported | Feature included or supported | Feature included or supported | Feature not included |
| Terminal Services Gateway | Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature partially supported | Feature included or supported | Feature included or supported | Feature not included |
| Terminal Services RemoteApp | Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature partially supported | Feature included or supported | Feature included or supported | Feature not included |
| Terminal Services Web Access | Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature partially supported | Feature included or supported | Feature included or supported | Feature not included |
| Plug & Play Device Redirection (Terminal Services) | Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature partially supported | Feature included or supported | Feature included or supported | Feature not included |
| Universal Description, Discovery, and Integration Services (UDDI)  | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| Web Server (Internet Information Services-IIS) | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Delegated Feature Management-IIS-not in IIS 6.0 | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Xcopy Deployment of Web Applications-IIS | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Failed Request Tracing-IIS -not in IIS 6.0 |  Feature partially supported | Feature partially supported | Feature partially supported | Feature partially supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Windows Deployment Services-WDS | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| Windows Media Services | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Hyper-V (Windows Server Virtualization) (requires x64 edition) | Feature not included | Feature partially supported | Feature partially supported | Feature partially supported[[1]](#footnote-2) | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| **Server Features** |
| Windows Activation Services | Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| BITS Server Extensions | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| Windows® BitLocker™ Drive Encryption | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Desktop Experience Pack | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| **High Availability Features** |
| Failover Clustering | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature not included |
| Create Cluster API | Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature not included |
| Cluster Migration Tool | Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature not included |
| Multi-siteClusters | Feature not included | Feature not included | Feature partially supported | Feature partially supported | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature not included |
| Hybrid Quorum Model | Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature not included |
| **Recover Features** |
| Windows Server Backup | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Bare Metal Recovery | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Internet Storage Naming Services | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| LPR Port Monitor | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| MSMQ Services | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Windows Network Load Balancing | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| Remote Assistance | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| RPC over HTTP Proxy | Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| Removable Storage Manager | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| SMTP Server | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| SNMP Service | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Storage Manager for SANs | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| Simple TCP/IP Services | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Subsystem for UNIX-Based Applications | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Telnet Client / Server |  Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| WINS Server | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Windows System Resource Manager | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported[[2]](#footnote-3) | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| Conditional Resource Allocation Policies | Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| SQL Server® Accounting Engine | Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| Microsoft .NET Framework 3.5 | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| Wireless LAN Service | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| SQL Server® 2005 Embedded Edition | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| **Event Viewer** |
| Event Viewer | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature partially supported |
| Windows Event Collector Service | Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| **Task Scheduler** |
| Task Scheduler | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| **File System and Storage** |
| Offline Client Side Caching | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| Storage Explorer | Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| Transactional File and Registry Operations |  Feature partially supported | Feature partially supported | Feature partially supported | Feature partially supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| On-demand file replication | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| iSCI Initiator |  Feature partially supported | Feature partially supported | Feature partially supported | Feature partially supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| Distributed file system (DFS)  | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| **Group Policy** |
| Group Policy | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Group Policy Preferences | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| **Hardware and Devices** |
| Hardware and Devices(Dynamic Partitioning) | Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature not included |
| **Initial Configuration** |
| Initial Configuration Tasks | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| **Microsoft Management Console** |
| Microsoft Management Console 3.0 | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| **Performance and Diagnostic Utilities** |
| Performance and Diagnostics Utilities | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature partially supported |
| Windows Memory Diagnostic Tools | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Performance and Reliability Monitor | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature partially supported |
| Data Collector Sets (Perfmon) | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature partially supported |
| **Platform Networking** |
| Platform Networking-IPv6 | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Platform Networking-Receive side scaling | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Enterprise QoS (quality of service) | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Secure sockets API | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Dead gateway protection | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Windows filtering platform | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| (TCP Offloading) | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Receive Window Auto-Tuning | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Black Hole Router Detection | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Network Diagnostics Framework | Feature partially supported | Feature partially supported | Feature partially supported | Feature partially supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| **Platform Security** |
| Platform Security | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Windows Firewall with Advanced Security | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Connection Security Role Wizard | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| Windows Service Hardening | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Device Installation Control |  |  |  |  | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| System File Protection | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| **Software Protection Platform**  |
| Software Protection Platform | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Key Management Service | Feature not included | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| Reduced Functionality Mode | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| **Server Core** |
| Server Core | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| **Server Manager** |
| Server Manager | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| Update Services | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Add Roles Wizard | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| Add Features Wizard | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| **Windows Management Instrumentation** |
| Windows Management Instrumentation | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| **Windows PowerShell** |
| Windows PowerShell [[3]](#footnote-4) | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature not included |
| **Remote** |
| Windows Remote Instrumentation (WinRM) | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Windows Remote Shell (WinRS) | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Authorization Manager |
| Authorization Manager | Feature not included | Feature included or supported | Feature included or supported | Feature included or supported |  Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |  Feature included or supported |
| **Identity Management for Unix** |
| Identity Management for UNIX | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| **Transactions** |
| Distributed Transaction Coordinator |  Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |
| Kernel Transaction Manager | Feature not included | Feature not included | Feature not included | Feature not included | Feature included or supported | Feature included or supported |  Feature included or supported | Feature included or supported | Feature included or supported |
| Remote Transaction Coordination | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported | Feature included or supported |  Feature included or supported |

# References

For more detailed information about these features in Windows Server 2008, see:

* [“Changes in Functionality from Windows Server 2003 with SP1 to Windows Server 2008](http://www.mytechlibrary.com/pages/windows-server-2008/changes_in_functionality_from_windows_server_2003_with_sp1_to_w.asp)” paper, published by Microsoft, in June 2007, authors Simon Farr and Carolyn Eller.
* “Windows Server 2008 Reviewers Guide”
* [Windows Server 2008 TechCenter](http://technet.microsoft.com/en-us/windowsserver/2008/default.aspx)
* FAQs about Windows Server 2008: <http://forums.microsoft.com/TechNet/ShowPost.aspx?PostID=432195&SiteID=17>
* Information about how Windows Server 2008 and Windows Vista work better together: <http://www.microsoft.com/windowsserver2008/better-together.mspx>
* Information about Windows PowerShell: <http://www.microsoft.com/windowsserver2003/technologies/management/powershell/default.mspx>
1. Microsoft Virtual Server 2005 R2 Service Pack 1 (SP1) provided virtualization functionality in Windows Server 2003. In Windows Server 2008, Hyper-V provides more extensive virtualization functionality. [↑](#footnote-ref-2)
2. Windows System Resource Manager is a free download available for Windows Server 2003 Enterprise Edition and Datacenter Edition. [↑](#footnote-ref-3)
3. Windows PowerShell is fully supported but is not included “out-of-the-box” and has to be downloaded and installed. [↑](#footnote-ref-4)