



Microsoft Windows Server 2003 R2 Overview Guide

*Microsoft Corporation
Published: December 2005*

Abstract

Microsoft® Windows Server™ 2003 R2 makes it easier and more cost-effective to extend connectivity and control to identities, locations, data and applications throughout and beyond an organization. Windows Server 2003 R2 is an update release of the award-winning Windows Server 2003 operating system. Built on Windows Server 2003 with Service Pack 1 (SP1), Windows Server 2003 R2 takes advantage of the stability and security enhancements of a proven code base while extending connectivity and control into new areas. Windows Server 2003 R2 offers all of the benefits of Windows Server 2003 with SP1 while greatly improving identity and access management, branch server management, storage configuration and management, and application development inside and outside your organization's boundaries. Windows Server 2003 R2 is easy to integrate into an existing Windows Server 2003 environment since it shares the same application compatibility, manageability, and serviceability as existing servers with Windows Server 2003 with SP1.

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.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2005 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, ActiveX, IntelliMirror, MSDN, MSN, Outlook, PowerPoint, SharePoint, Visual Studio, Windows, the Windows logo, Windows NT, Windows Server, and Windows Server System are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

- FIGURES..... VI**
- PRODUCT OVERVIEW..... 1**
 - Simplified Branch Server Management..... 1*
 - Simplified Identity and Access Management..... 2*
 - Efficient Storage Management..... 3*
 - Improved Web Platform 3*
 - Cost-Effective Virtualization 4*
- WINDOWS SERVER 2003 R2 PRIMER 5**
 - Release Philosophy 5**
 - Integration with Windows Server 2003 SP1 5**
 - About Windows Server 2003 SP1 5**
 - Updates..... 5*
 - Enhancements 6*
 - New features..... 6*
 - Why Should Organizations Deploy Windows Server 2003 SP1? 7**
 - Editions and Features 7**
 - System Requirements 8**
 - Getting Started with Windows Server 2003 R2..... 9**
 - To start Setup for a new installation from the product CDs..... 9*
 - To start Setup for a new installation from the network 9*
 - To start an upgrade on a computer running Windows Server 2003 (without SP1)..... 10*
 - To start an upgrade on a computer running Windows Server 2003 with SP1 10*
 - To start an upgrade on a computer running Microsoft Windows NT Server 4.0 or Microsoft Windows 2000 Server 11*
- TECHNICAL OVERVIEW 12**
 - Simplified Branch Office Server Management 12**
 - Branch Office 12*
 - Distributed File System 12*
 - Remote Differential Compression 12*
 - Distributed File System Replication 13*
 - Distributed File System Namespace 13*
 - Print Management Console..... 13*

Simplified Identity and Access Management	14
<i>Active Directory Federation Services</i>	14
<i>Classic Web SSO</i>	14
<i>Federated Web SSO.....</i>	14
<i>Federated Authorization and .NET Integration.....</i>	14
<i>Extensible architecture.....</i>	15
<i>Web Services interoperability.....</i>	15
<i>What Is ADFS: In-Depth Information.....</i>	15
<i>ADFS Requirements</i>	16
<i>Hardware requirements.....</i>	16
<i>Software requirements</i>	16
<i>Federation Service.....</i>	16
<i>Active Directory and ADAM account store requirements</i>	16
<i>Federation Service Proxy.....</i>	16
<i>ADFS Web Service Agent.....</i>	17
<i>Trusted certification authorities</i>	17
<i>TCP/IP network connectivity.....</i>	17
<i>DNS</i>	17
<i>Web server.....</i>	17
<i>Web browser.....</i>	17
<i>Active Directory Application Mode</i>	17
<i>ADAM Overview.....</i>	18
<i>What's new in ADAM</i>	18
<i>Microsoft directory technologies.....</i>	18
<i>Comparing ADAM to Active Directory.....</i>	19
<i>UNIX Identity Management.....</i>	19
Efficient Storage Management.....	20
<i>Storage Manager for SANs.....</i>	20
<i>LUN management for Fibre Channel subsystems</i>	20
<i>LUN management for iSCSI subsystems.....</i>	20
<i>File Server Resource Management</i>	21
<i>Storage Resource Manager quotas vs. NTFS disk quotas</i>	21
<i>Microsoft Services for Network File System.....</i>	21
Improved Web Platform.....	22
<i>Windows SharePoint Services.....</i>	22
<i>Applications for Windows SharePoint Services.....</i>	22

- SharePoint sites – file storage plus collaboration*..... 22
- SharePoint Central Administration – Web browser interface for managing servers*..... 23
- ASP.NET 2.0*..... 23
- Internet Information Services (IIS) 6.0* 23
- Cost-Effective Virtualization** **24**
- Additional Features** **24**
 - Web Services for Management*..... 24
 - Subsystem for UNIX-based Applications* 24
 - Support for 64-bit Applications* 25
 - Common Log File System*..... 25
 - MMC 3.0* 26
 - Action pane* 26
 - New Add/Remove Snap-in dialog box*..... 26
 - Improved error handling* 26
- SUMMARY**.....**27**
- RELATED LINKS****28**

Figures

Figure 1: Distributed File System 13

Product Overview

Microsoft Windows Server 2003 R2 makes it easier and more cost-effective to extend connectivity and control to identities, locations, data, and applications throughout and beyond your organization. Windows Server 2003 R2 is an update release of the award-winning Windows Server 2003 operating system. Built on Windows Server 2003 with Service Pack 1 (SP1), Windows Server 2003 R2 takes advantage of the stability and security enhancements of a proven code base while extending connectivity and control into new areas. Windows Server 2003 R2 offers all the benefits of Windows Server 2003 with SP1 while greatly improving identity and access management, branch server solutions, storage setup and management, and application development inside and outside your organization's traditional boundaries. Use Windows Server 2003 R2 to:

- **Simplify Branch Server Management:** Windows Server 2003 R2 allows you to maintain the performance, availability, and productivity benefits of a local branch office server while avoiding issues typically associated with branch office server solutions such as connectivity limitation and management overhead.
- **Improve Identity and Access Management:** Windows Server 2003 R2 includes Active Directory Federation Services, designed to help administrators address identity management challenges by making it possible for organizations to share a user's identity information more securely across security boundaries. R2 also provides UNIX password synchronization which helps integrate servers running Windows and UNIX by simplifying the process of maintaining secure passwords.
- **Reduce Storage Management Costs:** Windows Server 2003 R2 includes new tools designed to provide a centralized view of storage, simplified storage planning, provisioning and maintenance, and improved monitoring and reporting.
- **Provide a rich Web Platform:** Windows Server 2003 R2 enables businesses to extend their infrastructure over the Web while reducing development and management costs through the enhancements delivered with SP1, x64, Windows SharePoint Services, .NET Framework 2.0, and Internet Information Services 6.0.
- **Provide cost effective server virtualization:** Windows Server 2003 R2 Enterprise Edition will allow you to run up to 4 virtual instances of Windows Server 2003 R2 EE on one licensed physical server or hardware partition, thereby decreasing the costs for server virtualization.

Simplified Branch Server Management

Windows Server 2003 R2 delivers on the vision and provides the underlying technologies needed to simplify integration of branch office servers into a larger enterprise IT ecosystem. Windows Server 2003 R2 allows customers to maintain the performance, availability, and productivity benefits of a local branch office server while avoiding issues typically associated with branch office server solutions such as connectivity limitations and management overhead.

To achieve this vision, Windows Server 2003 R2 provides a branch office framework for the deployment and management of key server roles that are conceptually comprised in the following modes:

- **Optional.** Remote clients can failover from the local branch office server to another server — determined by closest site selection — if local services become unavailable. Clients automatically failback to a preferred server when services are restored.
- **Disposable.** The branch office server performs as a service cache that does not hold a unique state and does not require system backup. If the server fails, there is no impact on branch office functionality.

- **Replaceable.** If the branch server fails, it can be replaced, re-provisioned, or redeployed — server roles are well-adapted for branch offices and varying roles can be deployed as one. The recovery of data is automated.

Windows Server 2003 R2, the first in a wave of upcoming branch office technologies from Microsoft and industry partners, offers functionality that streamlines operations for remote file and print servers. Windows Server 2003 R2 features deliver distinct advantages for branch office integration through:

- **Robust File Replication** — Windows Server 2003 R2 includes a completely rewritten replication engine for the Distributed File System (DFS). DFS Replication (DFS-R) provides a robust multimaster file replication service that is significantly more scalable and efficient in synchronizing file servers than its predecessor, File Replication Services (FRS). DFS-R schedules and throttles replication schemes, supports multiple replication topologies, and utilizes Remote Differential Compression (RDC) to increase WAN efficiency. If WAN connections fail, data can be stored and forwarded when WAN connections become available.
- **Advanced Compression Technologies** — Remote Differential Compression (RDC) is a WAN-friendly compression technology that replicates only the changes needed to ensure global file consistency. RDC thus provides significant WAN efficiencies, including enhanced performance with replicated file size, an area of primary importance for branch office servers based on customer feedback.
- **Enhanced Management Tools** —
 - The Print Management Console (PMC) provides a richer view of a network's printer topology, enabling an IT administrator to monitor and react quickly to printer situations and thus allow seamless productivity for branch office print users. Ultimately, PMC allows branch servers to perform as print servers, due to the manageability benefits it provides.
 - Microsoft Management Console (MMC) 3.0 has been expanded to include an enterprise-wide administration framework for managing file and print services. Administrators will benefit from the familiar look and feel of Microsoft's standard management interface. Businesses can mitigate the need for on-site administrators or third-party consultants for resolving local issues.
 - The enhanced DFS Namespaces (DFS-N) user interface allows for easier management of file system roots within a network infrastructure, presenting shared folders to users as a grouping called a "Namespace."
 - In addition, Microsoft Operations Manager 2005 (MOM) Management Pack for DFS provides more granular management functions than FRS.
- **Centralized Data Stores** — Centralized data stores reduce the management costs of geographically disbursed mini data centers. The replication of branch office data is automated to a central location at specified intervals when there is available bandwidth. In this way round trips are minimized.
- **Increased End-User Productivity** — Branch servers provide reliable and consistent access to the latest data that end users and applications rely on. The server employs local data to handle local requests or central servers in the event that a local server becomes unresponsive.

Simplified Identity and Access Management

Organizations today are taking advantage of Web services to integrate their disparate internal applications. Furthermore, they are moving towards providing external users access to these internal applications. This allows organizations to better connect and collaborate with their customers, partners, and suppliers, helping to increase revenue growth, improve end-user satisfaction, and reduce operational costs.

Extending internal applications to external users presents IT with security and administration challenges. Organizations must be confident that only appropriate external users are provided access to company data, and that the access granted is consistent with the user's role. In addition, they must manage the increased administrative workload that commonly results from dramatically expanding the infrastructure user base.

Active Directory® Federation Services (ADFS) is a new feature in Windows Server 2003 R2 designed to help administrators address identity management challenges by making it possible for organizations to share a user's identity information securely across enterprise or organizational security boundaries. ADFS extends the value of Active Directory deployments to facilitate collaboration with partners, resulting in increased user productivity, greater IT efficiency, and better security. It also extends the value of Windows Server identity services in internet-facing Web environments, enabling stronger authentication for extranet deployments, native delegated administration, and close integration with Microsoft technologies.

In addition to ADFS, Windows Server 2003 introduces enhancements to Active Directory Application Mode (ADAM), as well as UNIX identity management features such as Server for Network Information Services, which helps integrate Windows® and UNIX-based Network Information Service (NIS); and Password Synchronization, which helps integrate servers running Windows and UNIX by simplifying the process of maintaining secure passwords.

Efficient Storage Management

To help accommodate the widely varying storage management capabilities found throughout the IT industry, Windows Server 2003 R2 includes new tools designed to provide 1) a centralized view of storage; 2) simplified storage planning, provisioning and maintenance; and 3) improved monitoring and reporting. These benefits are captured in convenient new tools that enable administrators to more efficiently manage storage across IT resources and optimize storage space on those resources. Storage management extends to two key new features contained in Windows Server 2003 R2:

- **File Server Resource Manager** – File Server Resource Manager (FSRM) enables system administrators to understand how storage is being used and to manage the use of their storage by generating storage reports, applying quotas to volumes and folders, and screening files on the server. Using FSRM you can better plan and optimize storage by creating quotas, creating file screens, and scheduling storage reports.
- **Storage Manager for SANs** – Storage Manager for SANs enables customers to provision storage on one or more storage subsystems on a storage area network (SAN). Based on Microsoft Virtual Disk Service (VDS) technology, Storage Manager for SANs allows provisioning on Fibre Channel and Internet SCSI (iSCSI) storage subsystems.

Improved Web Platform

Windows Server 2003 R2 delivers on the vision and provides the underlying technologies needed to deliver a secure, scalable Web Platform. Windows Server R2 delivers on the promise to enable businesses to extend their infrastructure over the Web while reducing development and management costs through the enhancements delivered with Windows Server 2003 SP1, x64, Windows SharePoint Services, .NET Framework 2.0, and Internet Information Services 6.0.

As organizations seek to take advantage of the great potential of the web-enabled enterprise, they are challenged to extend their business infrastructure to deliver:

- Effective collaboration across and beyond organizational boundaries.
- Efficient development of rich applications that scale with their needs.
- Lower cost of management and maintenance of Web infrastructure.

Windows SharePoint Services delivers a cost effective collaboration solution that can be deployed, configured, and managed quickly and at very low cost.

ASP.NET enables fast development of rich, DSI-ready Web Services and Applications using the .NET Framework included in Windows Server 2003 R2. .NET Framework 2.0 simplifies and accelerates configuration, deployment, and management of secure, scalable Web applications.

IIS 6 delivers a secure, high-performance Web server that is significantly enhanced by technology offered in Windows Server 2003 R2. Highest possible security is ensured by a built in security advisor. Downtime and errors are greatly reduced with improved debugging capabilities. Finally, x64 supportability allows IIS to deliver more performance for less money.

Cost-Effective Virtualization

With Windows Server 2003 R2 Enterprise Edition, each software license allows you to run, at any one time, one instance of the server software in a physical operating system environment and up to four instances of the server software in virtual operating system environments. These new use rights enable customers to save costs by using virtualization to consolidate their servers. In order to run the additional instances in a virtual operating system environment, you must also license virtualization software, such as Microsoft Virtual Server 2005. The licensing change, allowing up to four instances, is specific to Windows Server 2003 R2 Enterprise Edition. For the Standard Edition of Windows Server 2003 R2, you may only run one instance in either the physical or virtual environment. For the Datacenter Edition of Windows Server 2003 R2, in addition to running one instance of the software in a physical operating system environment per hardware partition on a licensed server, you may run one instance of the software in a virtual operating system environment per licensed processor on that server. For more detailed information on the license terms for Windows Server R2, check the following resources on this page. For licensing questions on the Datacenter Edition of Windows Server, contact your OEM that licenses Datacenter Edition with your server hardware.

What's New in Windows Server R2 Licensing?

<http://www.microsoft.com/windowsserver2003/howtobuy/licensingr2/overview.aspx>

Volume Licensing Product Use Rights

<http://www.microsoft.com/licensing/resources/downloads/default.aspx>

Windows Server 2003 R2 Primer

Release Philosophy

Packaging the new functionality of Windows Server 2003 R2 as a 2-CD release distinct from Windows Server 2003 SP1 helps organizations deploy only the new features they need to specific servers. The first CD in the release package contains a slipstream installation of Windows Server 2003 with SP1, and all of the Windows Server 2003 R2 features are contained on the second CD. Unlike deploying a service pack, organizations can select the new functionality they will adopt without forgoing any critical security updates. Moreover, as organizational needs change, they can install or uninstall the new features of Windows Server 2003 R2 as they see fit.

Integration with Windows Server 2003 SP1

Windows Server 2003 R2 is built on Windows Server 2003 SP1 to create the tightest possible integration, forming the best Windows Server operating system produced by Microsoft to date. Such integration means that while Windows Server 2003 R2 delivers powerful new functionality in the arenas of branch office server administration, identity management, and efficient storage management, it does not require testing above and beyond the testing required for SP1, lowering the costs of adoption. Application compatibility with SP1 means that there is application compatibility with Windows Server 2003 R2. Future updates can be released for both Windows Server 2003 SP1 and Windows Server 2003 R2, lowering the cost of administering network environments where both operating systems are being used.

About Windows Server 2003 SP1

Windows Server 2003 SP1 provides convenient, comprehensive access to the latest updates, enhancements, and new features for Windows Server 2003. Each of these components allows customers to better leverage the enhanced security, reliability, and performance of Windows Server 2003.

Updates

Update management is one of the great challenges of computer security. Despite the inherent management difficulties they present, updates will continue to play a vital role in better securing enterprise IT. While enhancements and new functionality delivered by Windows Server 2003 SP1 make great strides toward more proactive security, reacting to known threats is still a core mission of SP1.

Frequent updating is essential to keeping up with exploits as they are discovered. By providing these updates together in SP1, Microsoft provides customers, both new and old, with the latest protection for Windows Server 2003.

The updates disseminated by SP1 cover some of the most basic functionality—and thus remove some of the most widely exploited attack points—of Windows Server 2003. These updates include:

- **Microsoft Internet Explorer**—Updates to this software help prevent unintentional downloads of misrepresented, malicious code and the automatic resizing of browser windows as a ruse to extract sensitive data from employees.
- **Microsoft Outlook® Express**—This update affords users the option of rendering e-mail in plain text rather than HTML. This provides one more barrier against the spread of malicious code through e-mail.
- **WebDAV Redirector**—By updating this behind-the-scenes program, customers can access Web-based Distributed Authoring Versioning (WebDAV) servers, such as Microsoft Windows SharePoint® Services and MSN® Communities, as if they were standard file servers. Moreover,

this update helps prevent customers' credentials (user name, password) from being transmitted over unencrypted channels during such exchanges.

Microsoft addresses update-related server down time with the Hot Patching feature in SP 1. Hot Patching allows customers to apply updates to drivers, DLLs, APIs, or any non-kernel-level component of Windows Server 2003 *without restarting the server*.

Enhancements

In addition to finding and updating security holes before hackers can exploit them, SP1 includes improvements to functionality that originally shipped with Windows Server 2003. Such enhancements make a great product better and raise the security, reliability, and productivity of Windows Server 2003. Below are brief descriptions of some of these key enhancements:

- **Stronger defaults and privilege reduction on services**—Services such as RPC and DCOM are integral to Windows Server 2003, but they are also an alluring target for hackers. By requiring greater authentication for RPC and DCOM calls, SP1 establishes a minimum threshold of security for all applications that use these services, even if they possess little or no security themselves.
- **Support for “no execute” hardware**—SP1 allows Windows Server 2003 to utilize functionality built in to computing hardware to help ensure that malicious code cannot launch attacks from areas of computer memory that should have no code running in it. For both 32-bit and 64-bit systems, this enhancement closes the door on one of the broadest and most exploited avenues of information attack.
- **Network Access Quarantine Control components included**—Windows Server 2003 SP1 now includes the Rqs.exe and Rqc.exe components to make deployment of Network Access Quarantine Control easier.
- **IIS 6.0 metabase auditing**—The metabase is the XML-based, hierarchical store of configuration information for Internet Information Services (IIS) 6.0. The ability to audit this store allows network administrators to see which user accessed the metabase in case it becomes corrupted.

New features

As part of SP1, Microsoft is introducing powerful new functionality to Windows Server 2003.

- **Windows Firewall**—Also released with Windows XP Service Pack 2, Windows Firewall is the successor of the Internet Connection Firewall. Windows Firewall is a host (software) firewall, a firewall helping protect each client and server computer on a customer's network. Unlike Windows XP Service Pack 2, Windows Firewall is off by default on Windows Server 2003 Service Pack 1, and must be turned on to begin protecting systems. Windows Firewall is enabled by default for a brief time immediately following operating system installations that include Service Pack 1. Windows Firewall stays enabled for the duration of the new Post-Setup Security Updates portion of setup.
- **Post-Setup Security Updates (PSSU)**—Servers are vulnerable in the time between initial installation and having the latest security updates applied. To counter this, Windows Server 2003 with Service Pack 1 uses Windows Firewall to help block all inbound connections to the server after installation until Windows Update delivers the latest security updates to the new computer. After updating, Windows Firewall is turned off until it is manually configured for server roles. PSSU also guides users through immediate configuration of Automatic Updates.
- **Security Configuration Wizard (SCW)**—SCW is a wizard that configures server security based upon existing server roles. SCW asks questions about server roles and then stops all services not necessary to perform those roles. SCW does not add roles, but configures the server around the roles it performs. Like boarding up unused doors, this new feature helps reduce the attack surface of Windows Server 2003.

Why Should Organizations Deploy Windows Server 2003 SP1?

Windows Server 2003 SP1 is a no-cost means for enterprises to enhance Windows Server 2003. SP1 updates known vulnerabilities in Windows Server 2003 and adds additional complementary features and capabilities to enhance its security, reliability, and performance.

- **Enhanced security**—SP1 dramatically reduces the attack surface of Windows Server 2003. Not only does it reactively address known security holes through updates, it equips customers with the tools they need to face future security threats proactively. By shifting security into a role-based paradigm, SP1 makes it easy for customers to run only the services they need, eliminating the unnecessary services that can become potential footholds for hackers and malicious code. Moreover, role-based security eases the deployment of future updates, reducing the time it takes for IT professionals to prepare for attempted exploitation of newly discovered vulnerabilities.
- **Enhanced reliability**—Security is at the heart of IT reliability: a system plagued by external attack is by definition not reliable for any who depend upon it. By protecting against past threats and anticipating future threats, SP1 increases the reliability of Windows Server 2003.
- **Enhanced productivity**—Resources spent dealing with the aftermath of an attack or maintaining cumbersome security arrangements are resources siphoned away from the customer's core business. SP1 addresses this intersection of security and productivity. By aggressively countering security threats, SP1 reduces organizations' need to clean up after attacks; by simplifying and rationalizing update management, SP1 allows organizations to redirect resources from the security front to more appropriate use in their core businesses.

In addition to being a prerequisite for installing Windows Server 2003 R2, SP1 is especially attractive for organizations that have not yet adopted Windows Server 2003. Windows Server 2003 with SP1 incorporates all current updates and includes new functionality to address real-world needs discovered since the launch of Windows Server 2003. SP1 represents a milestone in the maturity of Windows Server 2003 and it forms the platform for Windows Server 2003 R2.

Editions and Features

Windows Server 2003 R2 Editions and Features			
Features	Standard Edition	Enterprise Edition	Datacenter Edition
File Server Resource Manager	√	√	√
Storage Manager for SANs	√	√	√
Active Directory Federation Services (ADFS)		√	√
ADFS Proxy		√	√
ADFS Web Agents	√	√	√
Active Directory Application Mode	√	√	√
Distributed File System – Replication with Remote Differential Compression	√	√	√
Distributed File System – Cross-File Remote Differential Compression*		√*	√*
Print Management Console	√	√	√
Microsoft Management Console 3.0	√	√	√

Windows Server 2003 R2 Editions and Features			
Features	Standard Edition	Enterprise Edition	Datacenter Edition
Windows SharePoint Services V2 SP2	√	√	√
.NET Framework 2.0	√	√	√
Subsystem for UNIX Applications	√	√	√
UNIX Interop (NIS Server, Password Sync, NFS Admin, etc)	√	√	√
x64 Availability	√	√	√
WS-Management	√	√	√

*Only one of the replication partners is required to be an Enterprise Edition or Datacenter Edition.

System Requirements

In general, system requirement for Windows Server 2003 R2 are the same as the following general Windows Server 2003 system requirements:

Windows Server 2003 R2 System Requirements			
Requirement	Standard Edition	Enterprise Edition	Datacenter Edition
Minimum CPU Speed	133 MHz	<ul style="list-style-type: none"> • 133 MHz for x86-based computers • 733 MHz for x64-based computers 	<ul style="list-style-type: none"> • 400 MHz for x86-based computers • 733 MHz for x64-based computers
Recommended Minimum CPU Speed	550 MHz	733 MHz	733 MHz
Minimum RAM	128 MB	128 MB	512 MB
Recommended Minimum RAM	256 MB	256 MB	1 GB
Maximum RAM	<ul style="list-style-type: none"> • 4 GB for x86-based computers • 32 GB for x64-based computers 	<ul style="list-style-type: none"> • 64 GB for x86-based computers • 1 TB for x64-based computers 	<ul style="list-style-type: none"> • 128 GB for x86-based computers • 1 TB for x64-based computers
Multiprocessor Support	Up to 4	Up to 8	<ul style="list-style-type: none"> • Minimum 8-way capable machine required • Maximum 64
Disk Space for Setup	1.5 GB	<ul style="list-style-type: none"> • 1.5 GB for x86-based computers • 2.0 GB for x64-based computers 	<ul style="list-style-type: none"> • 1.5 GB for x86-based computers • 2.0 GB for x64-based computers

Getting Started with Windows Server 2003 R2

As described earlier, the Windows Server 2003 R2 operating system is comprised of two product installation CDs. The first installation CD contains Windows Server 2003 with SP1. The second installation CD contains the components specific to Windows Server 2003 R2. Both CDs use the same product key. You can install Windows Server 2003 R2 either locally from the product CDs, or from your network.

To start Setup for a new installation from the product CDs

1. Determine whether the computer on which you want to start Setup can be started from the CD-ROM drive and whether you want to perform a new installation (not an upgrade). Continue only if both are true.
2. Insert the first CD in the drive, and then restart the computer.
3. Follow the instructions in your computer's startup routine to start the computer from the CD.
4. Wait for Setup to display a dialog box, and then follow the Setup instructions.

Important

When you are prompted to enter the product key, enter the product key that comes with the Windows Server 2003 R2 installation CDs. Entering this product key now ensures that you will not be prompted to enter a product key again later, during installation of the second CD.

5. After you set up Windows Server 2003 with SP1, log on to the computer with your administrator password. You are then prompted to insert the second CD.
6. Follow the Setup instructions.

To start Setup for a new installation from the network

1. On a network server, create a shared resource called \\servername\share, where servername is the name of your server, and share is the name of the shared resource that you are creating.
2. Copy the i386 folder from the first CD to the shared resource.
3. Copy the folder named "Cmpnents" from the second CD to the shared resource.

Note

The shared resource now contains two folders: \\servername\share\i386 and \\servername\share\cmpnents.

4. On the computer on which you want to install Windows Server 2003 R2, connect to the shared folder that contains the Setup files. Navigate to the i386 folder and click **winnt32.exe**.
5. Wait for Setup to display a dialog box, and then follow the Setup instructions.

Important

When you are prompted to enter the product key, be sure to enter the product key that has been provided to you for Windows Server 2003 R2. By entering this product key, you will not be prompted to enter a product key again later, during the second half of the installation.

6. After Setup for Windows Server 2003 with SP1 is complete, log on to the computer with your administrator password. The second half of the installation for components specific to Windows Server 2003 R2 starts automatically.
7. Follow the Setup instructions.

Notes

- When installing the operating system, if for some reason a product key that belongs to a different copy of Windows Server 2003 is entered, the operating system installation will complete

successfully. However, when you log on to the computer for the first time after you install the operating system itself, installation of the components contained on the second CD, on which the components specific to Windows Server 2003 R2 are located, will not start automatically. You will need to insert the second CD or reconnect to the shared network resource that contains the Setup files, navigate to the \components\R2\ folder, and click **setup2.exe** in order to finish installation of Windows Server 2003 R2. Setup will prompt again for the End User License Agreement (EULA), and a product key. When this occurs, the product key provided for Windows Server 2003 R2 must be entered.

- When the second CD is installed, Windows Server 2003 R2 resource files are simply loaded on the server in a location that will enable you to install them later, but the components themselves are not installed. After Windows Server 2003 R2 is set up, individual Windows Server 2003 R2 components can be installed using **Add or Remove Programs**, and selecting **Manage Your Server (MYS)/Configure Your Server (CYS)**.
- If the computer on which Windows Server 2003 R2 is installed is a domain controller but the Active Directory schema version is earlier than the Windows Server 2003 R2 schema version, the following error message will be displayed:

Setup cannot continue because the schema version of this domain controller is not compatible with Windows Server 2003 R2. Before you can install Windows Server 2003 R2, you must upgrade the schema version to Windows Server 2003 R2. Before you can successfully install Windows Server 2003 R2 on any of the Windows Server 2003 domain controllers in this forest, you must first upgrade the Active Directory schema. To upgrade the schema, on the schema operations master, run Adprep.exe /forestprep. The Adprep.exe command-line tool is available in the Cmpnents\r2\adprep directory on the Windows Server 2003 R2 installation CD. For a list of criteria for upgrading or for more information about extending the schema, see Help and Support.

If you receive this error message, you must upgrade the Active Directory schema before you can proceed.

To start an upgrade on a computer running Windows Server 2003 (without SP1)

1. Apply SP1 to your current version of Windows Server 2003.
2. Insert the second CD, which contains the components specific to Windows Server 2003 R2 in the drive, and wait for Setup to display a dialog box.
3. Follow the Setup instructions.

Notes

- When you are prompted to enter the product key, be sure to enter the product key that comes with the two installation CDs included in the Windows Server 2003 R2 release package.
- Before upgrading your current version of Windows Server 2003 to Windows Server 2003 R2, you must apply SP1 to that version. Otherwise, when you insert the second CD, the following error message is displayed:

Setup cannot run on this version of Windows. You must run Setup on a computer with Windows Server 2003 with Service Pack 1 or later installed.

To start an upgrade on a computer running Windows Server 2003 with SP1

1. Insert the second CD, which contains the components specific to Windows Server 2003 R2 in the drive, and wait for Setup to display a dialog box.
2. Follow the Setup instructions.

To start an upgrade on a computer running Microsoft Windows NT Server 4.0 or Microsoft Windows 2000 Server

1. You can also upgrade to Windows Server 2003 R2 from the following operating systems:
 - Windows NT® Server 4.0 with Service Pack 5 or later
 - Windows NT Server 4.0, Terminal Server Edition, with Service Pack 5 or later
 - Windows 2000 Server
2. Insert the first CD in the drive, and wait for Setup to display a dialog box.
3. Follow the Setup instructions.

Important

When you are prompted to enter the product key, be sure to enter the product key that comes with the two installation CDs included in the Windows Server 2003 R2 release package.

4. After Setup for Windows Server 2003 with SP1 is complete, log on to the computer with your administrator password. You are prompted to insert the second CD.
5. Follow the Setup instructions.

Technical Overview

Simplified Branch Office Server Management

Branch Office

Windows Server 2003 R2 provides technologies that assist in simplifying branch office management for the following scenarios:

- Publishing files from centralized hubs to branch offices.
- Replicating files from branch to hub locations for backup, fault tolerance, or cross-branch publishing.
- Loose collaboration of documents between branches or between hubs and branches.
- Efficient management of printers in branch offices, including drivers and queue management.

These scenarios are supported by the Distributed File System (DFS) solution, which includes new tools for DFS Namespaces, a new replication engine known as DFS Replication, and enhanced print management tools.

Distributed File System

The Distributed File System (DFS) solution in Windows Server 2003 R2 provides simplified, fault-tolerant access to files and WAN-friendly replication. Distributed File System consists of two technologies:

- DFS Namespaces, formerly known as Distributed File System, allows administrators to group shared folders located on different servers and present them to users as a virtual tree of folders known as a namespace. A namespace provides numerous benefits, including increased availability of data, load sharing, and simplified data migration.
- DFS Replication, the successor to File Replication service (FRS), is a new state-based, multimaster replication engine that supports scheduling and bandwidth throttling. DFS Replication uses a new compression algorithm known as Remote Differential Compression (RDC). RDC is a differential over-the-wire protocol that can be used to efficiently update files over a limited-bandwidth network. RDC detects insertions, removals, and rearrangements of data in files, enabling DFS Replication to replicate only the deltas (changes) when files are updated.

Remote Differential Compression

RDC is an advanced WAN-compatible compression technology that optimizes data transfers over limited-bandwidth networks. Instead of transferring similar or redundant data repeatedly, RDC accurately identifies file “deltas” and transmits only the differences to achieve bandwidth savings. This means, for example, the “deltas” caused by a simple title change in a 3 megabyte (MB) PowerPoint® presentation would take less than one second to replicate over a WAN, in contrast to one minute or more for the entire file.

RDC can also copy any roughly similar file from any client or server to another using data that is common to both computers. This effectively reduces the size of the data sent and the overall bandwidth requirements for the transfer. Local differencing techniques — sometimes called “patching” — compute the differences between two local files, detecting insertions, removals, and rearrangements of data. The differences can then be used to transform the old version to a new version. The differences between two known versions of a file are calculated on a server, and then sent to the client.

Microsoft’s internal RDC performance testing suggests that in some cases, bandwidth reduction factors may reach as high as 400:1.

Distributed File System Replication

DFS includes a highly scalable, multimaster state-based file replication service that synchronizes file servers. It supports:

- Automatic recovery from database loss or corruption.
- Scheduling and bandwidth throttling for replication schemes.
- Multiple replication topologies.

Distributed File System Namespace

DFS Namespaces allow administrators to group shared folders located on different servers and present them to users as a virtual tree of folders known as a namespace. A namespace provides numerous benefits, including increased availability of data, load sharing, and simplified data migration. Users can navigate these virtual namespaces without having to keep track of the names of the physical servers or shared folders hosting the data.

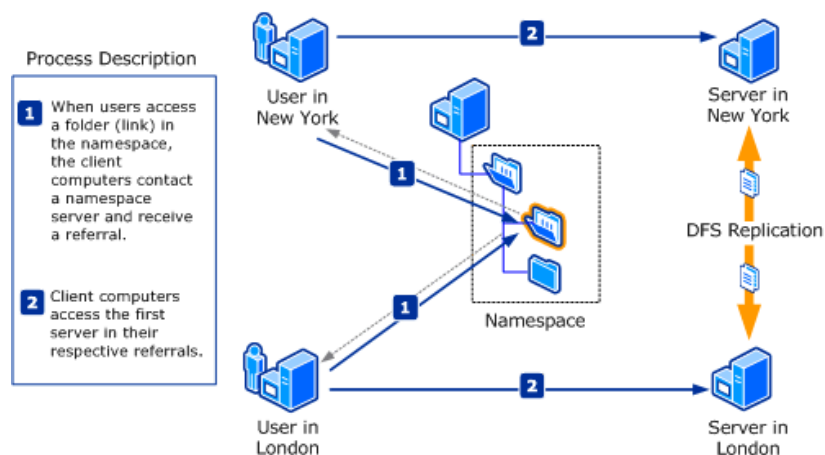


Figure 1: Distributed File System

If local servers become unavailable, DFS Namespace configurations provide for client failover by closest site selection and fallback to a preferred server. For example, DFS link that has targets in both the branch and the hub, branch clients will automatically failover to the hub when the local server is unavailable.

For Windows Server 2003 R2, DFS failback functionality allows administrators to set server priorities for root and link target referrals, including setting high and low priority servers. In this case, servers are first ordered by site cost and then by priority within each site. Clients failback to the branch server when availability is restored.

DFS Namespace is administered by using the DFS Management Console that provides a hierarchical view of namespace. The DFS Management Console incorporates functionality that was previously only available through command line interface (CLI). The DFS Management Console applies features from Microsoft Management Console (MMC) 3.0, including built-in HTML reports and diagnostics.

Print Management Console

Through the Printer Management Console (PMC), administrators have a central interface for managing all printers connected to all print servers within an organization. With PMC, administrators can monitor printer errors, deploy printer connections to clients, automatically find and install printers on a local branch office subnet, and run configuration scripts. PMC allows branch servers to perform as print servers because they are remotely manageable on a one-to-many basis.

PMC is an MMC snap-in that enables administrators to view and manage all the printers on every print server in administrators' organization from any computer on the network running Windows Server 2003 R2. PMC provides up-to-the-minute details such as the queue status, printer name, number of

jobs, driver name, and server name. By using the PMC filtering capability, administrators can set custom views. For example, administrators could view only those printers in a particular error state or only printers in a specific location that have more than one job in the queue.

Filtering by error state also allows administrators to manage multiple queues at once. For example, administrators can select more than one printer and then cancel, pause, or resume all the print jobs simultaneously. Administrators can also delete multiple printers at the same time.

The automatic detect feature finds and installs printers from the local subnet to the local print server. Administrators can log on to a branch location's local server by using Remote Desktop and use this feature to easily install printers remotely.

In cases where a printer has a printer Web page, PMC may display rich troubleshooting details such as exactly where a paper jam is happening or the printer's toner level. Some printer Web pages give the Administrator options for remote control functions that can help resolve problems at branch locations. By using the PMC, the printer Administrator may have a clearer picture of the problem before assistance is needed.

Simplified Identity and Access Management

Active Directory Federation Services

The fundamental purpose of Active Directory Federation Services (ADFS) is to take advantage of user single sign-on (SSO) technologies to authenticate a user to multiple, related Web applications over the life of a single online session. ADFS accomplishes this by securely sharing digital identity and entitlement rights, or "claims," across security and enterprise boundaries. The following are some of the key features of ADFS:

Classic Web SSO

Classic Web SSO scenarios involve cases where the user accessing an application are managed in an extranet directory collocated with the application. ADFS classic Web SSO features offer stronger authentication than conventional means through forms and client-side certificates, and a SSO cookie eliminates the need to re-authenticate for access to other applications in a federated application pool. This functionality, which has been provided by third parties in the past, is now integrated into the server platform with ADFS in Windows Server 2003 R2.

Federated Web SSO

With federation, the user authentication process (presenting and verifying credentials) takes place in a separate environment from the one where the application resides. ADFS enables federation of web applications, enabling customers, partners, and suppliers from different organizations to have a similar, streamlined user experience when they access another organization's Web-based applications with their own organization's credentials. Federation also works between business units or geographies within an organization.

Federated Authorization and .NET Integration

ADFS provides a rich model for building security tokens. The ADFS security token has the ability to carry data about users besides their identity, including user authorization/entitlement data.

These data, called *authorization claims* combined with the ability to transport the data securely in a security token, enables a feature called Federated Authorization. Rather than requiring the application administrator to entirely manage how users get access to specific application capabilities, Federated Authorization enables the delegated administration of users' access rights to trusted directory administrators.

At the application, ADFS integration with Windows Server technologies like ASP.NET Roles or Windows Authorization Manager (AzMan) provides end-to-end authentication and authorization management capabilities. Authorization Manager is a simple interface to provide application-level access to functionality through administrative mapping of incoming authorization claims to application roles and related application capabilities. Thus Authorization Manager, in combination with ADFS, help

to provide a roles-based access control (RBAC) environment for Windows-based internet-facing .NET Web applications.

Extensible architecture

ADFS provides an extensible architecture that supports various security token types, including Security Assertion Markup Language (SAML) 1.1 and Kerberos (as used in Windows Integrated Authentication). ADFS also offers the ability to perform *custom claims transformations* — for example, adding custom business logic from a database as a variable in an access request. Organizations can use this extensibility to modify ADFS to coexist with their current security infrastructure and business policies.

Web Services interoperability

ADFS provides a solution that is proven to interoperate with other security products that support the Web Services (WS-*) architecture. ADFS does this by employing the federation specification of WS-*, called WS-Federation. WS-Federation makes it possible for environments that do not use the Windows identity model to federate with Windows environments. Many identity management and security software vendors have demonstrated two-way interoperability with ADFS and plan to deliver complementary solutions to ADFS.

The WS-Federation Passive Requestor Profile (WS-F PRP) is an implementation of WS-Federation, which proposes a standard protocol for how passive requestors (such as Web browsers that support the widely used Hypertext Transfer Protocol (HTTP)) apply the federation framework. Within this protocol, Web service requestors are expected to understand the new security mechanisms and be capable of interacting with Web service providers.

Because ADFS is based on the WS-* architecture, it supports federated communications between any WS-enabled endpoints, currently including communications between servers and passive (HTTP/S) clients, such as Web browsers. In the future, ADFS will employ the WS-* architecture to expand its reach to Simple Object Access Protocol (SOAP)-based smart clients, such as servers, mobile phones, personal digital assistants (PDAs), desktop applications, and SOAP-based Web services.

What Is ADFS: In-Depth Information

Active Directory serves as a primary identity and authentication service in many organizations. Using Windows Server 2003 Active Directory, administrators can create forest trusts between two or more Windows Server 2003 forests to provide access to resources that are located in different business units or organizations. There are, however, scenarios in which forest trusts are not a viable option, for example two distinct organizations doing business across the internet, or applications located in DMZ or perimeter networks. (For more information about forest trusts, see "[How Domain and Forest Trusts Work](#)" in the [Windows Server 2003 Technical Reference](#) on the Microsoft Web site.

By employing ADFS, organizations can extend their existing Active Directory infrastructures to provide access to resources that are offered by trusted partners across the Internet, which can include external third parties or other departments or subsidiaries in the same organization. ADFS is tightly integrated with Active Directory, retrieving user attributes and authenticating users against Active Directory, as well as using Windows Integration Authentication and security tokens that are created by Active Directory.

ADFS works with both Active Directory and Active Directory Application Mode (ADAM). Specifically, ADFS can work with both enterprise-wide deployments of Active Directory or instances of ADAM. When it interacts with ADAM, ADFS uses Lightweight Directory Access Protocol (LDAP) Bind as a means to authenticate users. When it interacts with Active Directory, ADFS can take advantage of the strong authentication technologies in Active Directory, including Kerberos, X.509 digital certificates, and smart cards.

ADFS supports distributed authentication and authorization over the Internet, and ADFS can be integrated into an organization's or department's existing access management solution to translate the terms used within an organization into terms that are agreed on as part of a federation. ADFS can

create, secure, and validate the claims moving between organizations, and it can also audit and monitor the activity between organizations and departments to ensure secure transactions.

ADFS Requirements

ADFS requires the following hardware and software components.

Hardware requirements

- Processor speed: 133 MHz for x86-based computers or 733 MHz for x64-based computers
- Recommended minimum RAM: 256 MB
- Free disk space for ADFS setup: 10 MB

Software requirements

ADFS relies on server functionality that is built into the Windows Server 2003 operating system. The Federation Service, Federation Service Proxy, and ADFS Web Service Agent components cannot run on earlier operating systems. This section describes the software requirements for each ADFS component and the overall software configurations that are necessary for ADFS in a network environment.

Note that the Federation Service, Federation Service Proxy, and ADFS Web Service Agent can coexist on the same physical systems in the Release Candidate (RC) version of ADFS.

Federation Service

Computers running the Federation Service must have the following software installed:

- Windows Server 2003 with SP1
- Internet Information Server (IIS)
- ASP.NET
- Microsoft .NET Framework 2.0 Beta
- A default Web site that is configured with Transport Layer Security and Secure Sockets Layer (TLS/SSL)
- A certificate for the Federation Service. Note that because this certificate is used for signing tokens, it must be a digital signing X.509 certificate.

Active Directory and ADAM account store requirements

ADFS requires the presence of user accounts in Active Directory or Active Directory Application Mode (ADAM) for the account Federation Service. Active Directory domain controllers or computers hosting the account stores must have the following software installed:

- Windows Server 2003 with SP1
- Or
- Windows 2000 with Service Pack 4 (SP4) and critical updates

Note: Local accounts and Windows NT domain accounts cannot be used for user accounts in ADFS account stores.

Federation Service Proxy

Computers running the Federation Service Proxy must have the following software installed:

- Windows Server 2003 with SP1
- IIS
- ASP.NET

- Microsoft .NET Framework 2.0 Beta
- A default Web site configured with TLS/SSL

ADFS Web Service Agent

Computers running the ADFS Web Service Agent must have the following software installed:

- Windows Server 2003 with SP1
- IIS
- ASP.NET
- Microsoft .NET Framework 2.0 Beta
- A default Web site configured with TLS/SSL

Note that ADFS will not enable 128-bit encryption over SSL connections during setup.

Trusted certification authorities

Because TLS/SSL relies on digital certificates, certification authorities (CAs) such as Microsoft Certificate Services are an important part of ADFS. A CA is a mutually trusted third party that confirms the identity of a certificate requestor (usually a user or computer) and then issues the requestor a certificate. The certificate binds the requestor's identity to a public key. CAs also renew and revoke certificates as necessary.

For example, if a client is presented with a server's certificate, the client computer might try to match the server's CA against the client's list of trusted CAs. If the issuing CA is trusted, the client verifies that the certificate is authentic and has not been tampered with.

TCP/IP network connectivity

For ADFS to function, TCP/IP network connectivity must exist between the client, the domain controller, and the computers hosting the Federation Service, the Federation Service Proxy, and the Web server.

DNS

The internal Domain Name System (DNS) servers on the intranet forest must be configured to return the canonical name (CNAME) of the internal server that is running the Federation Service for authenticating users that are located in the intranet. For best results, do not use Hosts files with DNS.

Web server

For The RC version of Windows Server 2003 R2, only a machine running IIS 6.0 with ASP.NET is supported as a Web server.

Web browser

Although any current Web browser with JavaScript enabled should work as an ADFS client, only Internet Explorer 6.0, Internet Explorer 5.0 or 5.5 for older operating systems, Safari on Apple Macintosh, and Mozilla are supported for the Release Candidate.

Active Directory Application Mode

Active Directory Application Mode (ADAM) is an independent mode of Active Directory, without infrastructure features, that provides directory services for applications. It provides a data store and services for accessing the data store. It uses standard application programming interfaces (APIs) for accessing the application data. ADAM operates either as a stand-alone data store, or with replication. Its independence enables local control and autonomy of directory services for specific applications. It also facilitates independent, flexible schemas and naming contexts.

ADAM Overview

For organizations that require flexible support for directory-enabled applications, Microsoft has developed ADAM. ADAM is a Lightweight Directory Access Protocol (LDAP) directory service. Administrators can run ADAM on servers running Windows Server 2003.

ADAM can also run on clients running Microsoft Windows XP Professional. To run do so, administrators must install the latest service packs and hot fixes.

ADAM provides data storage and retrieval for directory-enabled applications, without the dependencies that are required for the Active Directory directory service. ADAM provides much of the same functionality as Active Directory, but it does not require the deployment of domains or domain controllers. Administrators can run multiple instances of ADAM concurrently on a single computer, with an independently managed schema for each ADAM instance.

What's new in ADAM

The following features are new to ADAM in Windows Server 2003 R2:

- Users can be created in the configuration partition so that ADAM users can be ADAM administrators.
- **Active Directory to ADAM Synchronizer tool.** This tool synchronizes objects from Active Directory to an ADAM instance. For more information, see Synchronize Data from Active Directory to an ADAM Instance and Adaminstall.
- ADAM users can bind to an ADAM instance by using digest authentication. This authentication method uses the default credentials of the server applications and eliminates the need to keep a plaintext version of the application's password in memory. Digest bind is supported in LDP.
- **Active Directory Schema Analyzer tool.** This tool helps with migrating the Active Directory schema to ADAM.
- **Newer version of LDP tool.** The updated tool includes an access control list (ACL) editor.
- **User Password Chaining.** ADAM can now chain user password requests in ADAM to the user object in Active Directory so that a password is changed in both directory services. When a user in ADAM who is also a user in Active Directory attempts to change the user password in ADAM, that change is treated the same as a user password change in Active Directory. Both the old and new password must be provided (except for Active Directory administrators, who only need to supply the new password), and the new password must meet any password policies that are set in Active Directory. Active Directory performs all policy checking.

Microsoft directory technologies

With the introduction of ADAM, Microsoft provides a choice of directory services. Both ADAM and Active Directory build on the same core Microsoft directory service technologies, but they address different needs within an organization.

Active Directory. Active Directory provides directory services for both the Windows network operating system (NOS) and for directory-enabled applications. For the NOS, Active Directory stores critical information about the network infrastructure, users and groups, network services, and so on. In this role, Active Directory must adhere to a single schema throughout an entire forest.

ADAM. ADAM provides directory services specifically for directory-enabled applications. ADAM does not require or rely on Active Directory domains or forests. However, in environments where Active Directory exists, ADAM can use Active Directory for the authentication of Windows security principals.

ADAM and Active Directory can run concurrently on the same network. In addition, ADAM can support both domain and workgroup users simultaneously.

Comparing ADAM to Active Directory

The following table illustrates the functional differences and similarities between ADAM and Active Directory.

Feature	ADAM	Active Directory
Supports multiple schemas per server	Yes	No
Supports multiple directory instances per server	Yes	No
Runs on Windows XP Professional	Yes	No
Runs on member servers	Yes	No
Supports X.500 naming for top-level directory partitions	Yes	No
Supports installing, starting, and stopping without a reboot	Yes	No
Group Policy	No	Yes
Global catalog	No	Yes
IntelliMirror [®] desktop management	No	Yes
Automated software distribution	No	Yes
Domain trusts and forest trusts	No	Yes
Public key infrastructure (PKI)/X.509	No	Yes
Supports DNS service (SRV) resource records	No	Yes
Supports Lightweight Directory Access Protocol (LDAP) application programming interface (API)	Yes	Yes
Supports Active Directory Service Interfaces (ADSI) API	Yes	Yes
Supports Messaging API (MAPI)	No	Yes
Delegated administration	Yes	Yes
Multimaster replication	Yes	Yes
InetOrgPerson	Yes	Yes
LDAP over Secure Sockets Layer (SSL)	Yes	Yes
Attribute-level security	Yes	Yes
LDAP access control list (ACL) support	Yes	Yes
Microsoft Identity Integration Server 2003 compatibility	Yes	Yes
Extensible schema	Yes	Yes
Supports application directory partitions	Yes	Yes
Supports installation of a replica from media	Yes	Yes
Supports 64-bit servers	Yes	Yes
Supports concurrent LDAP binding	Yes	Yes

UNIX Identity Management

Windows Server 2003 R2 provides Windows and UNIX integration with the following updated identity management solutions. These solutions help provide uninterrupted user access and efficient management of network resources across operating systems:

- **Server for NIS** helps integrate Windows and UNIX-based Network Information Service (NIS) servers by enabling an Active Directory domain controller to act as a master NIS server for one or more NIS domains. Identity Management for UNIX includes an easy-to-use wizard that a Windows domain administrator can use to export NIS domain maps to Active Directory entries. Once this is

done, an Active Directory domain controller running Server for NIS becomes the master server for the NIS domain.

- **Password Synchronization** helps integrate Windows and UNIX servers by simplifying the process of maintaining secure passwords. With Password Synchronization, users do not need to maintain separate passwords for their Windows and UNIX accounts or remember to change the password in multiple locations. Password Synchronization automatically changes a user password on the UNIX network when the user changes his or her Windows password, and vice versa.

Identity Management for UNIX makes it easy to integrate computers running Windows into an existing UNIX enterprise. Active Directory network administrators can use Server for NIS to manage Network Information Service (NIS) domains, and Password Synchronization will automatically synchronize passwords between Windows and UNIX operating systems.

With minor differences, Identity Management for UNIX is compliant with Internet Engineering Task Force (IETF) standard Request for Comments (RFC) 2307, meaning that a network's password and NIS attributes can be resolved by the Lightweight Directory Access Protocol (LDAP).

Password Synchronization supports Sun Solaris version 8 running on x86-based computers and Scalable Processor Architecture (SPARC)-based computers; Solaris version 9 running on SPARC-based computers; Hewlett Packard HP-UX version 11i; IBM AIX version 5L 5.2; and Red Hat Linux versions 8 and 9 running on x86-based computers and 64-bit AMD-based computers. Server for NIS should work with any operating system or product that uses LDAP.

Efficient Storage Management

Storage Manager for SANs

Storage Manager for SANs (SMfS) is a Microsoft Management Console snap-in that administrators can use to create and manage the logical units (LUNs) that are used to allocate space on storage arrays in both Fibre Channel and iSCSI environments. Administered through a conventional snap-in, Storage Manager for SANs can be used on storage area network (SAN) based storage arrays that support Virtual Disk Server (VDS) using a hardware VDS provider. Because of hardware, protocol, transport layer and security differences, configuration and LUN management differ for the two types (iSCSI and Fibre Channel) of supported environments. This feature will work with any type of Host Bus Adapter (HBA) or switches on the SAN. A list of VDS providers that have passed the Hardware Compatibility Tests (HCT) is available on www.microsoft.com/storage.

LUN management for Fibre Channel subsystems

On a Fibre Channel storage subsystem, LUNs are assigned directly to a server, which accesses the LUN through one or more Host Bus Adapter (HBA) ports. The administrator needs only to identify the server that will access the LUN, and enable one or more HBA ports on the server to be used for LUN I/O traffic. When the server is assigned to a LUN, the server can immediately access the LUN to create, augment, delete, and mask (or unmask) the LUN.

Support for multiple I/O paths. If a server supports Microsoft Multipath I/O (MPIO), Storage Manager for SANs can provide path failover by enabling multiple ports on the server for LUN I/O traffic. To prevent data loss in a Fibre Channel environment, make sure that the server supports MPIO before enabling multiple ports. (On an iSCSI subsystem, this is not needed: the Microsoft iSCSI initiator (version 2.0) that is installed on the server supports MPIO.)

LUN management for iSCSI subsystems

Unlike on a Fibre Channel storage subsystem, LUNs on an iSCSI subsystem are not directly assigned to a server. For iSCSI, a LUN is assigned to a *target* – a logical entity that contains one or more LUNs. A server accesses the LUN by logging on to the target using the server's iSCSI initiator. To log on to a target, the initiator connects to *portals* on the target; a subsystem has one or more portals, which are associated with targets. If a server's initiator is logged on to a target, and a new LUN is assigned to the target, the server can immediately access the LUN.

Securing data on an iSCSI SAN. To help secure data transfers between the server and the subsystem, configure security for the login sessions between initiators and targets. Using Storage Manager for SANs, you can configure one-way or mutual Challenge Handshake Authentication Protocol (CHAP) authentication between the initiator and targets, and you can also configure Internet Protocol security (IPsec) data encryption.

File Server Resource Management

With the increasing demand on storage resources as organizations rely more heavily on data than ever before, IT administrators face the challenge of overseeing a larger and more complex storage infrastructure, while at the same time tracking the kind of information it contains. Managing storage resources has come to include not only data size and availability but also the enforcement of company policies and a very good understanding of how existing storage is utilized. This allows for sound strategic planning and proper response to organizational changes.

File Server Resource Manager (FSRM) is Microsoft Management Console snap-in that encompasses a suite of tools that allows administrators to understand, control, and manage the quantity and type of data stored on their servers. By using File Server Resource Manager, administrators can place quotas on volumes, actively screen files and folders, and generate comprehensive storage reports. This set of advanced utilities not only helps the administrator efficiently monitor existing storage resources, but also aids in the planning and implementation of future policy changes.

You can use FSRM to perform the following tasks:

- Create quotas to limit the space allowed for a volume or folder and to generate notifications when the quota limits are approached and exceeded.
- Create file screens to filter the files that users can save on volumes and in folders and to send notifications when users attempt to save blocked files.
- Create periodic or storage reports that allow you to identify trends in disk usage and to monitor attempts to save unauthorized files.

FSRM console consists of two snap-ins: Storage Resource Management, which is used to create quotas that place size limits on folder trees and to create file screens that are used to block files from volumes and folders, and Scheduled Storage Tasks, which is used to schedule several types of storage reports and to generate reports. You can also configure e-mail notifications to be sent when quota limits approach or when users attempt to save files that have been blocked.

Using the FSRM console you can also manage storage resources on a remote computer. While you are connected, the results pane for that snap-in displays the objects created on the remote computer, allowing you to manage them from the console. In order to use FSRM remotely, the remote computer must also be running Windows Server 2003 R2, with the Storage Manager component installed. FSRM also supports servers that are clustered.

Storage Resource Manager quotas vs. NTFS disk quotas

The Windows 2000 and Windows Server 2003 operating systems support disk quotas, which are used to track and control disk usage per user on NTFS volumes. The following table outlines the advantages of using the quota management tools in Storage Resource Manager.

Quota features	Storage Resource Manager	NTFS disk quotas
Quota tracking	By folder or by volume	Per user on a volume
Disk usage calculation	Actual disk space	Logical file size
Notification mechanisms	E-mail, custom reports, command execution, event logs	Event logs only

Microsoft Services for Network File System

Microsoft Services for Network File System (MSNFS) provides Windows-based implementations of both the client and server aspects of Network File System (NFS), as well as related services and

utilities. The primary purpose of MSNFS is to provide an interoperability solution for enterprise businesses that have both Windows-based and UNIX-based clients. MSNFS supports the Network File System (NFS) protocol and provides file sharing interoperability between Windows and UNIX machines. It also provides a strategy for migrating from mixed or UNIX-based client environments to Windows. Moreover, MSNFS is now an integrated part of Windows Server.

MSNFS can provide:

- 64-bit support
- Better interoperation between Server Message Block (SMB) and NFS systems
- Improved reliability
- Support for NFS Devices (MKNOD)

Improved Web Platform

Deliver secure and scalable Web applications, extend business infrastructure over the Web and control costs via enhancements in Windows SharePoint Services, .NET Framework 2.0, x64 and Internet Information Services 6.0. Windows SharePoint Services enables efficient collaboration with employees, partners, and suppliers across organizational boundaries. ASP.NET 2.0, a component of the .NET Framework, makes Web Services and Applications easier to develop, deploy, configure & manage while Internet Information Services 6.0 delivers a secure, high-performance Web server that reliably extends Business Infrastructure to the Web.

Windows SharePoint Services

Microsoft Windows SharePoint Services is an integrated portfolio of collaboration and communication services designed to connect people, information, processes, and systems both within and beyond the organizational firewall. Windows SharePoint Services, Service Pack 2 (SP2), is included in Windows Server 2003 R2. Now administrators can install Windows SharePoint Services directly from the Configure Your Server or Manage Your Server Wizard.

With the Windows SharePoint Services, you are able to accelerate deployment and ultimately reduce IT administration costs on your collaboration platform.

Applications for Windows SharePoint Services

Microsoft Windows SharePoint Services can be easily customized using application templates. Application templates are tailored to address the needs and requirements for specific business processes or sets of tasks for organizations of any size. The applications are the first out-of-box custom scenarios for the Windows SharePoint Services platform, though they also provide a starting point for partners and developers looking to build deeper Windows SharePoint Services solutions.

SharePoint sites – file storage plus collaboration

Web sites based on Windows SharePoint Services provide a place where teams can communicate, share documents, and work together on a project. SharePoint functionality includes:

- Team collaboration features including event calendars, contacts, Web links, discussions, issues lists, and announcements.
- Document libraries – places where users can store and retrieve documents while taking advantage of rich features such as check-in and check-out, version history, custom metadata, and flexible, customizable views.
- Web Parts which can provide data access, Web services, and many other applications and content to SharePoint sites.

Site users can contribute to the site by using nothing more than a Web browser. However, if users have Windows SharePoint Services-compatible client programs, such as Microsoft Office 2003,

installed on their computers they can work seamlessly with the site, saving files to libraries, editing documents in the client program, and moving or linking that information to the site.

SharePoint Central Administration – Web browser interface for managing servers

Administrators can manage a single server or an entire server farm running Windows SharePoint Services from a Web browser interface called SharePoint Central Administration. Use SharePoint Central Administration to extend a virtual server, create sites (or turn on Self-Service Site Creation so users can create their own sites), manage security settings, manage the list of servers in a server farm, and so on. If administrators prefer, they can also use the Stsadm.exe command-line utility to manage their servers running Windows SharePoint Services.

ASP.NET 2.0

ASP.NET 2.0 reduces development and management costs of Web applications with improvements that simplify management, enable high performance solutions, and empower developers.

- Efficiently managing ASP.NET 2.0 Web sites and applications is simpler. A new configuration API allows administrators to write scripts that automate provisioning, deployment, and management. Additionally, a new MMC plug-in integrated with IIS 6.0 enables GUI-based administration of all ASP.NET configuration settings giving the user with integrated set of management tools for IIS and ASP.NET administration. With the Health Monitoring API, developers can add granular event-level analysis functionality to their applications which enables real-time tracing and stats of running applications.
- ASP.NET 2.0 introduces a number of new features for implementing high performance solutions. First, Web Sites can now be pre-compiled to enhance performance and responsiveness or to protect intellectual property by deploying with source code stripped away. Second, ASP.NET 2.0 offers features like an enhanced logging framework and built-in automated security and database caching which allow developers to build self-managing, self-healing applications on the DSI ([Dynamic Systems Initiative](#)) model. Lastly, ASP.NET 2.0 can be customized for any enterprise environment by replacing or extending any of the built-in features or services.
- New ASP.NET services and built-in features enable more productive development of richer application scenarios. Forty five new Security, Data, Navigation & Web Part Controls allow developers to write up to 70% less code for faster development of rich web sites and applications. Security is enhanced and streamlined by Membership and Login APIs adding custom authentication and authorization to new applications. Additionally, a new page design framework using Master Pages, Themes, and Skins separates site design from code and content to deliver a consistent, customizable user experience that can be updated and maintained separately from the application's code and content.

Internet Information Services (IIS) 6.0

The Web Platform delivered in Windows Server 2003 R2 is anchored on IIS 6.0, a secure scalable web server that is enhanced by Windows Server 2003 technologies specifically SP1 and x64 supportability. These technologies help decrease infrastructure costs by reducing downtime & errors, improving security, and increasing performance & scalability.

- Event Tracing for Windows, Metabase Auditing and WC3 Centralized Logging tools added to IIS in SP1, simplify debugging defective applications or improper configurations with their powerful log and trace capabilities.
- The Security Configuration Wizard in SP1 augments security lockdown already prevalent in IIS 6.0 with a graphical interface that walks IT Pros through a thorough hardening of the Web server.
- x64 support for IIS 6.0 reduces errors and downtime by decreasing cache recycling by doubling virtual memory available to 32 bit applications.

- IIS on x64 runs on significantly lower CPU and supports twice as many connections creating significant IT savings.

Cost-Effective Virtualization

With Windows Server 2003 R2, Microsoft has introduced a number of licensing changes to better facilitate virtualization. To begin with, a single license for Windows Server 2003 R2 Enterprise Edition grants the organization that holds it a license to that physical instance of the operating system **as well as** licenses for four **virtual** instances of either Windows Server 2003 R2 Standard Edition or Enterprise Edition. Moreover, Windows Server 2003 R2 licenses only apply to **running** instances of the operating system; an organization with a library virtual machines with Windows Server 2003 R2 installed on them would not pay for a license of for each installed instance (as with the traditional licensing model), rather, the customer would pay for only those instances of Windows Server 2003 R2 that were running at any given time. Thus not only does this new licensing model provide excellent value with Windows Server 2003 R2 Enterprise Edition, it also nurtures the adoption of virtualization by only making organizations pay for what they use.

Additional Features

Web Services for Management

Windows Remote Management Service is Microsoft's implementation of the new Web Services for Management protocol and allows organizations to use a secure and firewall-friendly remote management protocol.

Web Services for Management include the following benefits:

- Allows organization to use a secure and firewall friendly remote management protocol.
- Enables cross-firewall remote management of servers using WMI via HTTP and SOAP.
- Enables management of remote servers when the operating system is not running in a pre-boot and post-crash scenario such as a change boot order or power-cycle.

Hardware management makes Window Server aware of IPMI instrumentation in the motherboard with a new driver in the following scenarios:

- Events raised in the hardware system event log are also displayed in he Windows event log.
- Sensor values and probes can be read and set through a new WMI provider such as status of fan speed and temperature.
- Allows IPMI to be accessible to all management tools and scripts that use WMI.

Subsystem for UNIX-based Applications

Subsystem for UNIX-based Applications (SUA) is a source-compatibility subsystem for compiling and running custom UNIX-based applications on a computer running a Windows server-class operating system. Administrators can perfect their applications in SUA with little or no change to their original source code.

Subsystem for UNIX-based Applications provides an operating system for POSIX processes. SUA, along with its package of support utilities (such as shells and a Telnet client) available for download on the Microsoft Beta website, provides a complete UNIX environment. The download package includes a comprehensive set of scripting utilities and a software development kit (SDK) designed to fully support the development capabilities of SUA while providing a complete UNIX-based application development experience.

SUA also supports case-sensitive file names, job control, compilation tools, and the use of over 300 UNIX commands, utilities, and shell scripts. Because the subsystem installs separately from the Windows kernel, it offers true UNIX functionality without any emulation.

New features in this release include:

- **Database (OCI/ODBC) library connectivity.** SUA supports connectivity to Oracle and Microsoft SQL Server from database applications, through the Oracle Call Interface (OCI) and the Open Database Connectivity (ODBC) standard.
- **Microsoft Visual Studio Debugger Extension for debugging POSIX applications.** SUA includes support for debugging the POSIX processes using the Visual Studio IDE.
- **Utilities based on SVR-5 and BSD UNIX environments.** The SUA download package supports two different UNIX environments: SVR-5 and BSD.

Support for 64-bit Applications

Using a process called thunking, SUA provides support not only for 64-bit applications running on a 64-bit operating system, but also default support for 32-bit binaries running on a 64-bit operating system.

Common Log File System

Common Log File System (CLFS) is a loadable driver that provides kernel-mode or user-mode applications with a robust logging subsystem. CLFS is a unique Windows technology that can be used to develop applications and middleware which depend on durably writing and reading sequential data. Examples include replication agents, auditing agents, databases, and other transactional resource managers.

Common Log File System features:

Ability to create log files with a single stream of data or with multiple streams of data for shared use by one or more clients

Circular and linear logging

Guaranteed ability to flush buffered data by pre-reserving space in the log

Policy-based log size and space management

Sharing of a single log by both kernel and user clients

Notification mechanism to allow different users within the same log to coordinate their log use

Flexible buffering of log data

Archiving APIs do not interfere with normal operations

Atomic multi-sector writes

Torn-write detection

Administrators can use CLFS for Windows to build reliable user-mode or kernel-mode components that run on a single system or in a server cluster environment. CLFS simultaneously supports one or more independent log files on a single system. Administrators can configure log files for dedicated use by a single client or for shared use by multiple clients. Log file accesses can either be directed to local disk or to disks on remote systems by using internal client/server support. Within a cluster, log files can fail over to another system using standard mechanisms.

CLFS is optimized for performance. All writes to the log file are buffered until an explicit flush, an opportunity to share a write with another client, or the buffer is filled. Log data is written directly to the hard disk from the log buffers without copying. Multiple streams of data can be written during the same I/O operation, resulting in only one disk seek for what normally takes multiple seeks and writes. Reads are cached to save disk accesses during normal operation or bursts of read activity.

MMC 3.0

Administrators can use Microsoft Management Console (MMC) to create, save, and open administrative tools (called snap-ins) that manage the hardware, software, and network components of their Windows operating system. MMC 3.0 can be run on Windows Server 2003 R2.

MMC does not perform administrative functions, but hosts tools that do. Snap-ins are the most common of these tools. Other items that administrators can add include Microsoft® ActiveX® controls, links to Web pages, folders, and tasks.

Windows Server 2003 R2 includes several preconfigured snap-in consoles, such as Event Viewer (Eventvwr.msc) and Performance Monitor (Perfmon.msc). Administrators can create additional snap-in consoles to meet their needs. Depending on how a snap-in console is configured, it can be a customizable multi-function tool for an IT generalist, a limited-function tool for delegating work to an IT specialist, or anything in between.

There are two ways that administrators can use MMC: in user mode, working with existing snap-in consoles to administer a system, or in author mode, creating new snap-in consoles or modifying existing snap-in consoles.

Microsoft Management Console (MMC) 3.0 supports richer functionality in snap-ins that are written to take advantage of the MMC 3.0 infrastructure. In addition, there are several improvements that apply to any MMC 3.0 console:

Action pane

The **Action pane** appears at the right-hand side of the MMC snap-in console. It lists the actions that are currently available to administrators, based on the currently selected items in the tree or the results pane.

To show or hide the action pane, click the **Show/Hide Action Pane** button in the toolbar, which is similar to the **Show/Hide Tree** button.

New Add/Remove Snap-in dialog box

The new **Add/Remove Snap-in** dialog box makes it easy to add, organize, and remove snap-ins. Administrators can control which extensions are available, and whether to automatically enable snap-ins that may be installed later. They can nest snap-ins and rearrange the snap-ins in the tree.

To use this dialog box in the RC version, administrators must manually set a registry key.

Improved error handling

MMC 3.0 notifies administrators of errors in snap-ins that could cause MMC to fail, and provides several options for responding to those errors.

Summary

Windows Server 2003 R2 makes it easier and more cost effective to extend connectivity and control to identities, locations, data and applications throughout and beyond your organization. Windows Server 2003 R2 is an update release of the award-winning Windows Server 2003 operating system. Built on Windows Server 2003 with Service Pack 1, Windows Server 2003 R2 takes advantage of the stability and security of a proven code base while extending connectivity and control into new areas. Windows Server 2003 R2 offers all the benefits of Windows Server 2003 with SP1 while greatly improving identity and access management, branch server management, storage setup and management, and application development inside and outside your organization's boundaries. Windows Server 2003 R2 is designed to be slipstreamed into existing Windows Server 2003 environments without retesting or recertifying existing roles or applications or upgrading to new Client Access Licenses, easing administrative burden and simplifying deployment and adoption. Windows Server 2003 R2 builds upon the increased security, reliability and performance provided by Windows Server 2003 with Service Pack 1 and demonstrates Microsoft's commitment to continuously improving the Windows Server platform.

Related Links

For more information on Windows Server 2003 R2, Windows Server 2003, and the Windows Server System™, see the following:

- “[Windows Server 2003](http://www.microsoft.com/windowsserver2003/)” on the Microsoft Windows Server 2003 Web site at <http://www.microsoft.com/windowsserver2003/>
- “[Windows Server System](http://www.microsoft.com/windowsserversystem/)” on the Microsoft Windows Server System Web site at <http://www.microsoft.com/windowsserversystem/>
- “[Windows Server 2003 R2](http://www.microsoft.com/windowsserver2003/R2/)” on the Microsoft Windows Server 2003 Web site at <http://www.microsoft.com/windowsserver2003/R2/>

For more information on Identity Management, see the following:

- “[Automate Information Access with Identity Management](http://www.microsoft.com/idm/)” on the Microsoft Windows Server System Web site located at <http://www.microsoft.com/idm/>
- “[Identity and Directory Services](http://www.microsoft.com/windowsserver2003/technologies/idm/)” on the Microsoft Windows Server 2003 Web site at <http://www.microsoft.com/windowsserver2003/technologies/idm/>
- “[Microsoft Identity and Access Management](http://www.microsoft.com/technet/security/topics/identitymanagement/idmanage/)” on the Microsoft TechNet Web site at <http://www.microsoft.com/technet/security/topics/identitymanagement/idmanage/>
- “[ADFS](http://msdn.microsoft.com/theshow/episode047/)” on the Microsoft MSDN® Web site at <http://msdn.microsoft.com/theshow/episode047/>
- “[Web Services Development Center](http://msdn.microsoft.com/webservices/)” on the MSDN Web site at <http://msdn.microsoft.com/webservices/>

For more information on Self-Managing Dynamic Systems see the following:

- “[Microsoft Announces Comprehensive Virtualization Strategy to Enable Self-Managing Dynamic Systems](#)” on the Microsoft PressPass Web site.