



Microsoft Windows .NET Server 2003 Family Reviewer's Guide

September 2002

Microsoft®

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

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 reviewers guide 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.

© 2002 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, IntelliMirror, JScript, MSN, the .Net logo, Outlook, Visual Basic, Visual C++, Visual Studio, Win32, Windows, the Windows logo, Windows Media, and Windows NT 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.

Abstract

Today, more than 60 percent of all servers shipped are shipped with Microsoft® Windows® Server.¹ Businesses, governments, and institutions worldwide have embraced the Windows Server platform for its superior business value, both in IT dependability and productivity as well as its sheer ability to be easily transformed among roles as business necessities require and as new opportunities present themselves.

Microsoft Windows .NET Server 2003 is the next step forward in the evolution of the Windows Server computing platform. This reviewer's guide is an in-depth look at important improvements and new features contained in Windows .NET Server 2003.

¹ Q2 FY '01 to Q2 FY '02 (Q4 CY '00 to Q4 CY '01). IDC Worldwide Quarterly Server Tracker, May 2002.

Contents

PRODUCT OVERVIEW.....	IX
Windows .NET Server 2003 Family Creates Value.....	ix
Windows .NET Server 2003 Family Editions:.....	x
WINDOWS .NET SERVER 2003 FAMILY PRIMER	1
Product Family Editions	1
Limited-Distribution Editions.....	1
System Requirements.....	3
System Capabilities	4
Getting Started with Windows .NET Server 2003	5
Manage Your Server Wizard.....	6
What's New and Different in Windows .NET Server 2003.....	7
Built for Dependability	7
Built for Productivity	7
Built for a Connected World	8
Built for Best Economics	8
Summary Table of What's New and Improved.....	9
What's .NET About Windows .NET Server 2003.....	12
What Has Microsoft Done about Security in Windows .NET Server 2003.....	12
TECHNICAL OVERVIEW	14
Active Directory	14
Introduction	14
Benefits	14
Features and Improvements	15
Improved Management and User Interface.....	21
Improvements and New Features in Group Policy	22
Summary.....	25
More Information.....	26
Application Services.....	27

Introduction	27
Benefits	27
New Features and Improvements	27
Summary.....	32
More Information	32
Clustering	33
Introduction	33
Benefits	33
New Features and Improvements	33
Server Cluster Features	34
Network Load Balancing Features	37
Summary.....	38
More Information	39
File and Print Services	40
Introduction	40
Benefits	40
New Features and Improvements	40
Enhanced File System Features	40
Improved Printing Features.....	43
Summary.....	44
More Information	44
Internet Information Services 6.0	45
Introduction	45
Benefits from Deploying IIS 6.0.....	45
New Features and Improvements	46
New Process Model	46
New Security Features.....	49
New Manageability Features.....	50
New Performance and Scalability Features	52
Enhanced Development Experience and New Programmatic Features	53
Platform Improvements	55
Summary.....	57

More Information	58
Management	59
Introduction	59
Benefits	59
New Features and Improvements	59
Additional Features	65
Summary.....	68
More Information	68
Networking and Communications	69
Introduction	69
Benefits	69
New Features and Improvements	70
Summary.....	77
More Information	77
Security.....	78
Introduction	78
Benefits	78
New Features and Improvements	79
Summary.....	84
More Information	84
Storage Management.....	86
Introduction	86
Benefits	86
New Features and Improvements	86
Summary.....	89
More Information	89
Terminal Services	91
Introduction	91
Benefits	91
New Features and Improvements	92
Summary.....	94
More Information	94

Enterprise UDDI Services.....	95
Introduction	95
Benefits	95
New Features and Improvements	96
Summary.....	98
Windows Media Services	99
Introduction	99
Scenarios	99
Features and Improvements	100
Dynamic Content Programming	100
Fast Streaming.....	100
Industrial Strength.....	101
Extensible Platform	101
Summary.....	102
FEATURE COMPARISON CHART	103
WINDOWS .NET SERVER 2003, WINDOWS XP PROFESSIONAL, AND MICROSOFT OFFICE XP: BETTER TOGETHER	106
Providing Dependable Technologies at a Reasonable Cost.....	106
<i>Windows .NET Server 2003.....</i>	<i>106</i>
<i>Microsoft Windows XP Professional with Office XP</i>	<i>107</i>
Enhancing Productivity with Easy to use Tools and Technologies	107
<i>Windows .NET Server 2003.....</i>	<i>107</i>
<i>Microsoft Windows XP Professional with Office XP</i>	<i>108</i>
Connecting Users, Customers and Partners Together.....	108
<i>Windows .NET Server 2003.....</i>	<i>108</i>
<i>Microsoft Windows XP Professional with Office XP</i>	<i>109</i>
Summary.....	109
RELATED LINKS	110

Product Overview

Customer implementations in some of the most requirement-intensive business and government information-technology environments, in every corner of the globe, established Microsoft's currently-shipping Windows 2000 Server as the clear business-value leader among server computing platforms. Indeed, for calendar year 2001, International Data Corporation calculated that, worldwide, more than 60 percent of all servers shipped were shipped with Windows Server-family systems—a number growing at double-digit rate for the previous several years.¹

Following on this legacy, the Microsoft Windows .NET Server 2003 Family is destined to demonstrate even higher levels of dependability, performance, and connectivity, with unprecedented price/performance value. Microsoft has built the considerable feedback of customers and third-party partners as well as the independent testing of thousands of individuals into the disciplined engineering development of the Windows .NET Server 2003 Family.

At the cornerstone is native-mode Microsoft .NET functionality through the .NET Framework and standards-based technologies, which will enable businesses to easily and seamlessly connect information, people, systems, and devices. Windows .NET Server 2003 is, to be sure, the foundation enabling an unprecedented level of software integration through the use of XML-based Web services.

Windows .NET Server 2003 Family Creates Value

Windows .NET Server 2003 operating system is the most productive infrastructure platform for powering connected applications, networks, and web services—from the workgroup to the data center.

Dependable – Customers will find the Windows .NET Server 2003 operating system provides a dependable, enterprise-ready computing environment that has significant improvements that take the next step forward in building on the core of reliability, availability, scalability, and security introduced in Windows 2000 Server.

Productive – Windows .NET Server 2003 enables greater productivity for both IT administrators and end-users. Improved IT deployment and management tools— particularly in the Active Directory® service —simplify processes for administrators, while enhancements such as Volume Shadow Copy Services greatly enhance end-user productivity.

Connected – Windows .NET Server 2003 is integral to the Microsoft .NET Web services vision. With networking improvements, integration of the .NET Framework and ASP.NET, improvements to Internet Information Services, and many more new and improved features, the Windows .NET Server 2003 Family provides the ideal platform to develop, deploy, and host Web services applications.

Best Economics – The Windows .NET Server 2003 Family builds on the strength of Windows 2000 Server, with evolutionary improvements that deliver a superior, cost-effective server, while providing an ideal computing platform for organizations of any size.

By building on the solid foundation of Windows 2000 Server, the Windows .NET Server 2003 operating system enables businesses to retain and even increase the value of their existing IT investments while lowering overall computing costs. Windows .NET Server 2003 is a great choice for companies that haven't yet upgraded from Windows NT® Server4.0. Upgrading to the Windows .NET Server 2003 Family brings the advantage of cutting edge performance and reliability, and it

interoperates well with earlier Windows-based server computers and domains, so an incremental upgrade plan is a secure option.

Windows .NET Server 2003 Family Editions:

- **Windows .NET Server 2003, Standard Edition**, is the dependable server operating system for everyday needs of businesses of all sizes
- **Windows .NET Server 2003, Enterprise Edition**, is the platform of choice for high reliability, performance, and superior business value; in 32-bit and 64-bit editions
- **Windows .NET Server 2003, Datacenter Edition**, is for business- and mission-critical applications that demand the highest levels of scalability and availability; in 32-bit and 64-bit editions
- **Windows .NET Server 2003, Web Edition**, is optimized for serving and hosting web pages

In order to support the demands of today's enterprises, an operating system has to achieve the highest levels of reliability, scalability and manageability and must interoperate smoothly with disparate systems. It has to do this while keeping costs as low as possible and providing a solid return on investment for the business.

Reliable – Windows .NET Server 2003 includes new and enhanced features to help servers and applications attain enterprise levels of reliability. Both Windows .NET Server 2003, Enterprise Edition, and Windows .NET Server 2003, Datacenter Edition, will support 8-node clustering. It also introduces enhanced Network Load Balancing (NLB) to help improve the performance of Web-based applications and services. Security is improved with introduction of the Common Language Runtime (CLR) and improvements to Kerberos support and Public Key Infrastructure.

Scalable – Windows .NET Server 2003 is designed to scale up and scale out to meet enterprise levels of demand. Windows .NET Server 2003, Enterprise Edition, and Windows .NET Server 2003, Datacenter Edition, will support up to 8 or 32 processors, respectively, and up to 128GB of RAM in the 64-bit version of Datacenter Edition. Windows .NET Server 2003 improvements to storage support will enable better performance, larger volume sizes and more files per volume than ever before, not to mention improvements to the Distributed File System (DFS) and support for booting from a Storage Area Network (SAN). Internet Information Services (IIS 6.0), the newest release of Windows web services, has improved scalability with better performance and reliability features.

Manageable – Windows .NET Server 2003 incorporates enterprise-class management features, including enhancements to Active Directory and Group Policy management, as well as new and improved command-line utilities and Windows Management Instrumentation (WMI). Windows .NET Server 2003 fully supports Remote Installation Services (RIS), making deployment simpler. Enhancements to the Active Directory Management Tool (ADMT) and to the Windows Installer make upgrades and installation easier and administrative tasks like configuring storage volumes and group policy are now simplified.

Interoperable – Windows .NET Server 2003 is compatible with many third party products, industry standards, all currently-supported Windows-family server and client operating systems, Microsoft Office, and other Microsoft business applications. Windows .NET Server 2003 domains maintain a high level of backward compatibility with Windows 2000 and Windows NT 4.0 computing environments

and domains. The Windows .NET Server 2003 Family includes more public APIs than any previous server version, to allow third-parties to take advantage of the power of the Windows .NET Server 2003 platform. Native support for XML and related technologies means that Windows .NET Server 2003 will interoperate with XML-based applications and services.

Windows .NET Server 2003 Family Primer

The Windows .NET Server 2003 Family of server operating systems represents the next step in the ongoing evolution of the Windows Server Family. Windows .NET Server 2003 builds on the proven reliability, scalability, and manageability of Windows 2000 Server, to deliver the most productive infrastructure platform for powering connected applications, networks, and web services—from the workgroup to the data center. Windows .NET Server 2003 unleashes the agility to quickly and efficiently meet the changing demands of today's business computing environment, while providing the high levels of dependability, scalability and security that customers expect from a full-featured server operating system.

Product Family Editions

The Windows .NET Server 2003 Family comprises four editions:

- **Windows .NET Server 2003, Standard Edition**—The dependable server operating system ideal for everyday needs of business of all sizes, providing the optimal solution for file and printer sharing, secure Internet connectivity, centralized desktop application deployment, and a rich connected environment among employees, partners, and customers.
- **Windows .NET Server 2003, Enterprise Edition**—The platform of choice for large enterprises as well as small and medium-size businesses to develop, deliver, and secure applications, Web services, and infrastructure—delivering high reliability, performance, and superior business value. Enterprise Edition will be available in both 32-bit and 64-bit editions.
- **Windows .NET Server 2003, Datacenter Edition**—This is the server of choice for business-critical and mission-critical applications that demand the highest levels of scalability and availability. Datacenter Edition will be available through the Datacenter Program in both 32-bit and 64-bit editions.
- **Windows .NET Server 2003, Web Edition**—Optimized for serving and hosting web pages, while maintaining the core functionalities that support enhanced reliability, manageability, and security.

Limited-Distribution Editions

Limited-distribution Windows Server editions based on the Windows .NET Server 2003 code have been available through selected OEMs since June 2001 and have enjoyed considerable success in their early release. Windows Advanced Server, Limited Edition is Microsoft's first 64-bit Windows server operating system supporting the Intel Itanium-based processors. It is based on the 64-bit code in Windows .NET Server 2003, Enterprise Edition, and is optimized for memory- or computational-intensive mechanical-design graphics, database, and scientific applications.

Similarly, Windows Datacenter Server, Limited Edition was based on the Windows .NET Server 2003, Datacenter Edition, code base. It is optimized as a high-performance release of 32-bit Windows Server designed for 16-way-capable servers or higher. Windows Datacenter Server, Limited Edition is intended for customers who require the highest levels of performance and scalability in online transaction processing (OLTP), online analytical processing (OLAP), data warehousing, and data mining.

Windows Datacenter Server, Limited Edition has posted three Transaction Processing Council TPC-C, non-clustered, Top-Ten records since its pre-release availability to OEMs and as of 15 June 2002

holds the No. 8 position on this prestigious list. Windows Datacenter Server, Limited Edition also holds the No. 1 position on the SAP-SD three-tier benchmark as of this date.

Both Windows Advanced Server, Limited Edition and Windows Datacenter Server, Limited Edition are fully tested and supported versions suitable for production in computing environments for which they are optimized. Customers who registered their limited-edition versions will receive without additional cost the corresponding 64-bit versions of Windows .NET Server 2003, Enterprise Edition, or Windows .NET Server, Datacenter Edition, when they are released. Support for the Limited Edition versions will be discontinued 90 days after the Windows .NET Server 2003 Family becomes commercially available.

System Requirements

Windows .NET Server 2003 Family System Requirements ¹				
Requirement	Web Edition	Standard Edition	Enterprise Edition	Datacenter Edition
Minimum CPU Speed	133 MHz	133 MHz	133 MHz for x86-based computers 733 MHz for Itanium-based computers	400 MHz for x86-based computers 733 MHz for Itanium-based computers
Recommended CPU Speed	550 MHz	550 MHz	733 MHz	733 MHz
Minimum RAM	128 MB	128 MB	128 MB	512 MB
Recommended Minimum RAM	256 MB	256 MB	256 MB	1 GB
Disk Space for Setup	1.5 GB	1.5 GB	1.5 GB for x86-based computers 2.0 GB for Itanium-based computers	1.5 GB for x86-based computers 2.0 GB for Itanium-based computers

¹System requirements are shown for RC1 only. Final system requirements are subject to change.

System Capabilities**Windows .NET Server 2003 Family System Supports²**

Requirement	Web Edition	Standard Edition	Enterprise Edition	Datacenter Edition
Maximum RAM	2 GB	4 GB	• 32 GB for x86-based computers • 64 GB for Itanium-based computers	• 64 GB for x86-based computers • 128 GB for Itanium-based computers
Multi-Processor Support	1 or 2	1 or 2	Up to 8	• Minimum 8 required • Maximum 32
Cluster Nodes	No	No	Up to 8	Up to 8

² System capabilities are shown for RC1 only. Final system requirements are subject to change.

Getting Started with Windows .NET Server 2003

Windows .NET Server 2003 setup and installation is similar to the setup process for Windows 2000 Server, so administrators with experience in Windows 2000 setup and deployment will be able to use their knowledge when setting up Windows .NET Server 2003. There are a number of important enhancements, however:

- **New Setup Wizard**—The new Setup Wizard for Windows .NET Server 2003 retains much of the design of the Windows 2000 Server Setup Wizard. This design has been enhanced, however, to make it easier to find setup-related tasks and information. The new Setup Wizard reflects the task-based design of Windows .NET Server 2003 by grouping common tasks with documentation and information to help administrators perform them.
- **Dynamic Update**—The Setup Wizard now gives users the option of downloading updated setup files and drivers from Microsoft. This option can also be scripted as part of an unattended setup.
- **Compatibility Check**—The Setup Wizard allows users to do a detailed compatibility test to their computer. They can also check the Microsoft web site for dynamic updates as part of the compatibility test process.

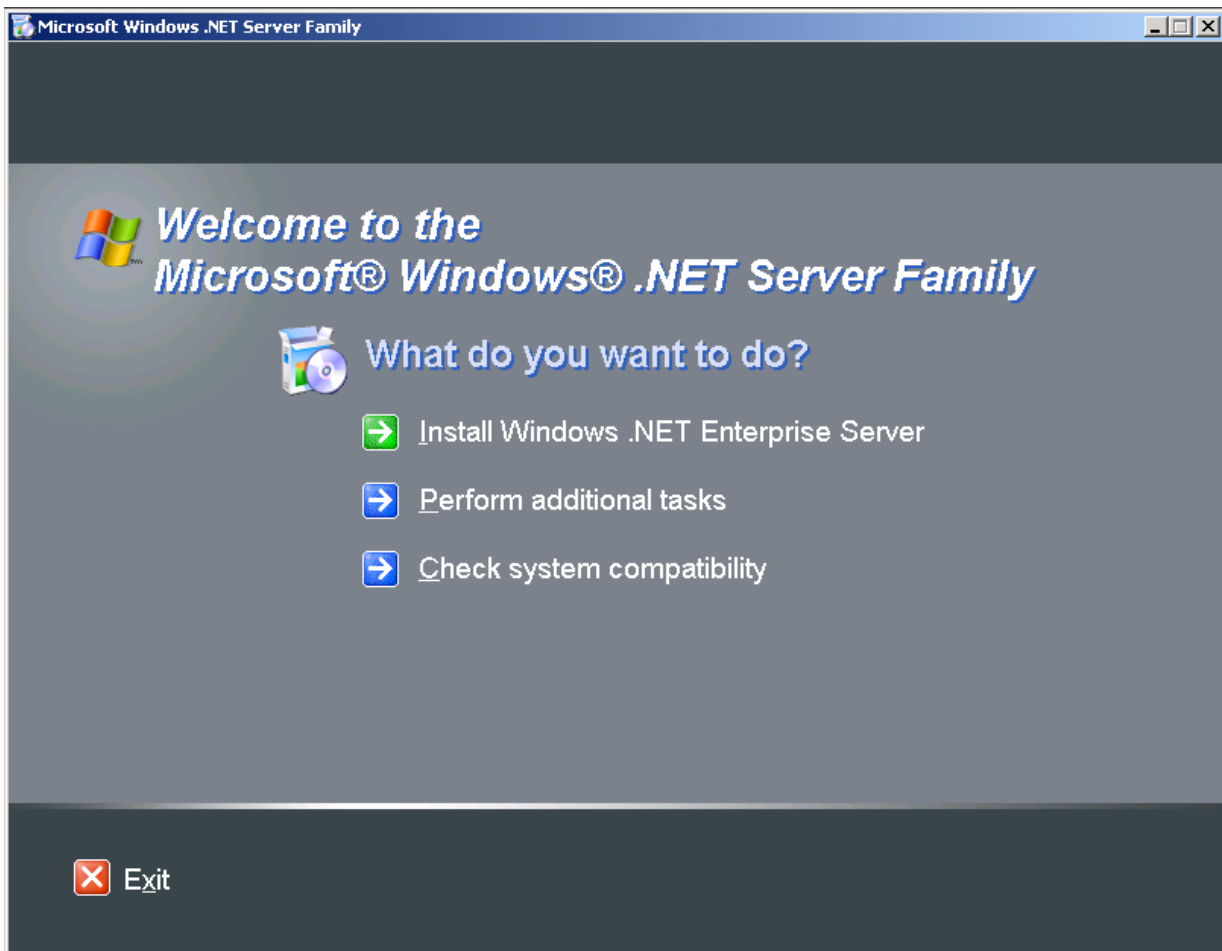


Figure 1 – Windows .NET Server 2003 Family Setup Wizard

Manage Your Server Wizard

The new Manage Your Server Wizard in Windows .NET Server 2003 replaces the Configure Your Server Wizard that was used in Windows 2000 Server. The Manage Your Server Wizard exposes common tasks that administrators need to carry out, as well as documentation and Help files to help complete those tasks (see figure 2). One of the main goals of the Manage Your Server Wizard is to allow administrators to set a server up to carry out a specific task, such as creating a domain controller, DNS server, DHCP server, Web server and so on. The wizard allows administrators to choose the role or roles which the server will fill and make configuration changes as appropriate for that role. The wizard also shows which roles already have been configured.

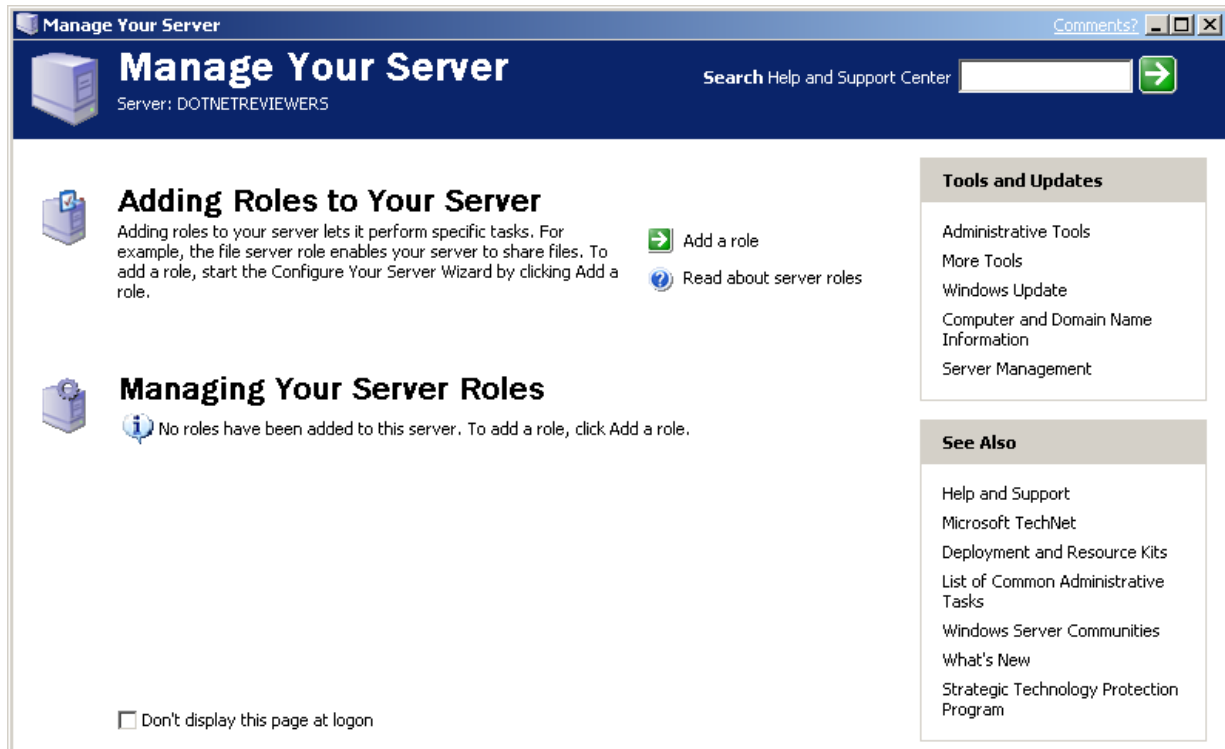


Figure 2 – Manage Your Server Wizard

What's New and Different in Windows .NET Server 2003

Over the past ten years, business's use of and reliance upon technology has changed dramatically. In a connected world today, software must meet dramatically new demands for availability, productivity, and connectivity from any place and on any device. Security standards which were fine in a world where networks were small and isolated are insufficient where systems must interconnect and communicate on a global scale.

Over the last several years, the power of PC-architecture has grown by leaps and bounds even as relative prices have plummeted. As companies gain access to new and more powerful, smaller computers, they demand correspondingly greater levels of performance and power from their software. At the same time, there has been a strong trend away from monolithic architectures that cannot adapt to change, toward distributed modular Web services and interoperable, agile systems that can be created quickly and altered as needs change. Finally, users demand technologies that let them communicate and collaborate effectively with people in the next office or on a different continent.

Windows .NET Server 2003 is a next generation server-side operating system designed to meet the needs of modern business. This doesn't mean that Microsoft has discarded what was best in Windows 2000 Server; rather, Windows .NET Server 2003 represents the natural evolution of the Windows Server Family. Windows .NET Server 2003 takes the technologies present in Windows 2000 Server and improves and streamlines them. In addition, Windows .NET Server 2003 adds a host of new features and technologies in response to customer demand and a changing world.

Built for Dependability

Today's businesses expect technology to be a consistent enabler of business value. They want systems that are always up and always responsive, and they demand a level of security that's appropriate to today's challenges. Windows .NET Server 2003 includes new features and improvements that render it the most dependable, enterprise-ready server operating system Microsoft has created to date while standing as an absolute reflection of Microsoft's commitment to trustworthy computing.

Microsoft has made improvements to technologies introduced in Windows 2000 Server, like Network Load Balancing (NLB), server clusters, and Active Directory. Microsoft is introducing new technologies like the new Common Language Runtime (CLR) to safeguard networks from malicious or poorly designed code. And Microsoft also has made leaps forward in the area of security with new and improved security for Internet Information Services (IIS) 6.0 as well as through PKI, Kerberos, and support for smart cards and biometrics.

Active Directory performance and flexibility now is faster and more robust over unreliable WAN connections thanks to more efficient synchronization and replication as well as caching of credentials in branch office domain controllers.

Built for Productivity

Companies look to computing technology to improve productivity across their businesses, from front-end knowledge workers who want powerful tools that are easier to use to back-end administrator services that are quick to deploy, easy to manage, and able to respond to need flexibly.

Windows .NET Server 2003 enables greater productivity for both IT administrators and end users thorough enhanced capabilities in system management and storage. Microsoft has made great strides

in evolving manageability in Windows .NET Server 2003. The new task-based design makes it easier to find and carry out common tasks. Improvements to the Microsoft Management Console (MMC) and to Active Directory improve performance and make management easier. Windows .NET Server 2003 introduces new management and administration features, including Domain Rename, cross-domain and cross-forest management, Metadirectory Management Services (MMS) and Resultant Set of Policy (RSOP). Enhanced Windows Management Instrumentation (WMI) providers and command-line tools for server tasks give administrators great granular control.

As well, to make storage and backup easier while at the same time significantly reducing the demands on system administrators' time, Windows .NET Server 2003 includes Volume Shadow Copy Services (VSS)—which provides point-in-time backups of networked shares—among the new and improved file services functionality. File and print services have been improved with the addition of the WebDAV remote document sharing technology. Enhancements to the Distributed File System (DFS) and Encrypting File System (EFS) allow for powerful, flexible file sharing and storage. Support for 64-bit printing and print clusters also has been added in Enterprise Edition and Datacenter Edition.

Enterprise Edition and Datacenter Edition offer support for 64-bit computing on supported hardware platforms, allowing faster completion of processor- and memory-intensive applications. Windows .NET Server 2003 supports Intel's Itanium and Itanium2 processors.

Built for a Connected World

Gone are the days when computing was done in a back room on a standalone PC or a small network. Today's networks are connecting intranets, extranets, and the Web. More and more companies are using the Internet to communicate with their customers and partners every day.

Networking improvements and new features in the Windows .NET Server 2003 Family extend the versatility, manageability and dependability of network infrastructures. Windows .NET Server 2003 allows users to more easily that ever stay connected to their infrastructure from anywhere and on any device. Microsoft has built significant networking enhancements in Windows .NET Server 2003, including Internet Protocol version 6 (IPv6), Point-to-Point Protocol over Ethernet (PPoE), and Internet Protocol Security (IPSec) over Network Address Translation (NAT).

Windows Media™ Services in Windows .NET Server 2003 provide a reliable, scalable means to deliver and manage dynamic content quickly and in a cost effective way. Windows Media Services make Windows .NET Server 2003 an ideal platform for distribution of streaming audio and video over corporate intranets and the Internet.

Perhaps most importantly, though, Windows .NET Server 2003 represents a revolutionary step forward in fashioning the ideal platform to develop, distribute, and host Web services created with Microsoft .NET. Windows .NET Server 2003 is optimized for hosting XML-based Web services thanks to native support of Microsoft .NET and XML with the inclusion of the .NET Framework. More about what's .NET about Windows .NET Server 2003 is included later in this section as well as throughout the document.

Built for Best Economics

Windows .NET Server 2003 has been designed to help companies build the value of their business while keeping costs down. The high reliability of Windows .NET Server 2003 helps control costs by reducing outages and downtime. Windows .NET Server 2003 has the flexibility to scale up and out in response to demand and the agility of the complete platform enables businesses to act on new

business needs as well as capitalize on emerging opportunities more quickly and effectively. Powerful management and configuration tools allow businesses to deploy and manage systems as easily and efficiently as possible, and compatibility with legacy and third party products means businesses won't lose their investment in existing infrastructure. The bottom line is a powerful, robust platform that helps build business value now and into the future.

Summary Table of What's New and Improved

Windows .NET Server 2003 builds on the foundation of Windows 2000 Server, improving on existing technologies by making them even more reliable and easier to use. In addition, it adds new features and technologies that expressly address the needs of today's businesses. The new and enhanced features and technologies of Windows .NET Server 2003 are summarized in the chart below. A more complete listing is shown in the expanded chart in the Feature Comparison section.

Explanation: ● = Feature included ◐ = Feature partially supported

Feature	Web Edition	Standard Edition	Enterprise Edition	Datacenter Edition
.NET Application Services				
.NET Framework ¹	●	●	●	●
Internet Information Services (IIS) 6.0	●	●	●	●
ASP.NET ¹	●	●	●	●
Enterprise UDDI Services ¹		●	●	●
Clustering Technologies				
Network Load Balancing	●	●	●	●
Server Clusters			●	●
Communications & Networking Services				
Virtual Private Network (VPN) Support	◐	●	●	●
Internet Authentication Service (IAS)		●	●	●

IPv6	●	●	●	●
Feature	Web Edition	Standard Edition	Enterprise Edition	Datacenter Edition
Directory Services				
Active Directory™	◐	●	●	●
Metadirectory Services (MMS) Support			●	
File & Print Services				
Distributed File System (DFS)	●	●	●	●
Encrypting File System (EFS)	●	●	●	●
Shadow Copy Restore	●	●	●	●
Removable and Remote Storage		●	●	●
Fax Service		●	●	●
Print Services for UNIX	●	●	●	●
Services for Macintosh		●	●	●
Management Services				
IntelliMirror	●	●	●	●
Resultant Set of Policy (RSOP)	●	●	●	●
Windows Management Instrumentation (WMI) Command Line	●	●	●	●
Remote OS Installation	●	●	●	●

Remote Installation Services (RIS)		●	●	●
Feature	Web Edition	Standard Edition	Enterprise Edition	Datacenter Edition
Multimedia Services				
Windows Media™ Services ¹		●	●	●
Scalability				
64-bit Support for Intel® Itanium™-Based Computers			●	●
Hot add memory ²			●	●
Non-Uniform Memory Access (NUMA) ²			●	●
Datacenter Program				●
Security Services				
Internet Connection Firewall ¹	●	●	●	
Public Key Infrastructure, Certificate Services, and Smart Cards	◐	●	●	●
Terminal Services				
Remote Desktop for Administration	●	●	●	●
Terminal Services		●	●	●
Terminal Services Session Directory			●	●

¹ Not supported in Windows .NET Server 2003, 64-bit edition operating system.

² May be limited by lack of support by OEM hardware.

What's .NET About Windows .NET Server 2003

The Microsoft .NET platform will enable business to take advantage of next generation business solutions that function in today's connected environment. Microsoft .NET is a set of technologies for building connected applications that tie information, people, systems and devices together. With .NET, companies can turn key business processes into xml-based Web services that can easily be aggregated into full business solutions. This allows businesses to adapt quickly to change and to leverage the power of the Internet in their day-to-day operations.

Windows .NET Server 2003 is a reliable, scalable high performance server platform that is ideally suited to enable businesses to create, distribute and host XML-based Web services. Windows .NET Server 2003 is fully integrated with the .NET Framework and offers native support for Web services standards like XML, SOAP, UDDI and WSDL. Microsoft Passport is integrated with Windows .NET Server 2003 authentication, providing a secure method of handing internet-based users.

Windows .NET Server 2003 increases developer productivity by giving developers access to powerful tools that let them create distributed services in the language of their choice. By giving developers more reusable objects, built-in services and powerful integration with the .NET Framework, Windows .NET Server 2003 will become the preferred platform for creating next generation Web technologies.

Enterprise UDDI Services provides standards-based Web Services infrastructure in Windows .NET Server 2003 to deploy a private UDDI service for intranet and extranet use. UDDI Services makes it easy to discover, share and re-use Web Services and other programmable resources, improving developer and IT productivity and resulting in a lower total cost of ownership (TCO) and more reliable and manageable applications.

In addition Windows .NET Server 2003 includes the latest release of Microsoft Internet Information Services (IIS). IIS 6.0 features greatly enhance performance and reliability. Web applications running on IIS 6.0 will scale more effectively to multi-processor computers, and better isolation and management of threads helps to ensure greater reliability. IIS 6.0 includes full integration with Active Server Pages .NET (ASP.NET), making it easier to create high performance Web services.

What Has Microsoft Done about Security in Windows .NET Server 2003

As companies extend and connect intranet and extranet sites, security becomes more important than ever. Customers are concerned about privacy and the integrity of their systems and data, and they expect software vendors to be accountable for the security of their products. The next generation server operating system must attain a new level of security and reliability. Microsoft has taken an industry-leading role in achieving a new level of reliability, security and stability with Windows .NET Server 2003.

Microsoft is committed to the vision of trustworthy computing. Simply put, trustworthy computing creates a framework in which computer-powered devices of all sorts can be as secure and trustworthy as the appliances you have in your own home. While this is a long-term goal, Windows .NET Server 2003 brings significant steps toward trustworthy computing today. This level of confidence doesn't just require cutting-edge security features, but also the management of code that runs in the environment, minimizing the damage caused by malicious or poorly written code. Ultimately, trustworthy computing will unite people, processes and products into a trusting framework for doing business.

Achieving a truly secure computing environment requires the effort of everyone involved, from administrators and end-users, to software developers and vendors. Microsoft Windows .NET Server

2003 is a reliable platform that provides the administrative tools, technologies and developer support that companies need to build better security and secure applications to meet today's standards. As part of its commitment to reliability security and dependable computing, Microsoft has reviewed every line of code underlying its Windows .NET Server 2003 Family as part of their enhanced effort to identify possible fail points and exploitable weaknesses. In addition, Windows .NET Server 2003 includes Secure Windows Update, so that companies can get the benefit of critical updates as they become available.

With Windows .NET Server 2003, Microsoft introduces the Common Language Runtime (CLR). The CLR is a software engine that helps ensure a secure runtime environment by reducing the number of bugs and security holes caused by common application-programming errors. This makes applications more reliable, leaves fewer vulnerabilities for malicious attackers to exploit, and protects the environment from untrustworthy code from outside sources. When a piece of code is ready to run, CLR checks to make sure that it can run without error, that the current security permissions are appropriate for it to run, and that the code does not carry out any actions that are inappropriate. The CLR keeps track of where code was downloaded from, if it was signed by a trusted developer, and if it has been altered in any way since it was signed.

Microsoft is introducing new security features in Windows .NET Server 2003, such as the Internet Connection Firewall (ICF) and software restriction policies. ICF is a software-based firewall that protects and monitors traffic across the boundary between the network and the Internet. Software restriction policies give administrators a policy-driven mechanism to identify programs running on computers in the domain, and control their ability to execute.

Microsoft also has enhanced security in the latest release of Internet Information Services. IIS 6.0 includes selectable cryptographic services, advanced digest authentication and configurable access control of processes. In addition, the Web server does not install automatically, and installs in lockdown mode by default. This provides a greater level of control over the security of back-end servers and Web sites.

Finally, Windows .NET Server 2003 includes improvements upon the industry-standard security technologies that Microsoft incorporated into Windows NT 4 and Windows 2000. Windows .NET Server 2003 includes technologies like Kerberos, Public Key Infrastructure (PKI) and Smart Card logon. The Encrypting File System (EFS) and Secure Sockets Layer (SSL) have been improved in Windows .NET Server 2003. Microsoft also has included integration with Microsoft Passport for Web-based authentication and security.

Technical Overview

The twelve subsections that follow provide an overview of key technologies and features included in Windows .NET Server, Enterprise Edition. The feature comparison chart in the following section enumerates features included in individual editions of the Windows .NET Server 2003 Family and identifies which are new and which represent improvements over features available in Windows 2000 Server.

Active Directory

Introduction

Active Directory is the directory service for Windows .NET Server 2003, Standard Edition, Enterprise Edition, and Datacenter Edition. It stores information about objects on the network and makes this information easy for administrators and users to find—providing a logical, hierarchical organization of directory information. This section provides an overview of benefits, new features, and improvements for Active Directory in Windows .NET Server 2003.

Benefits

Improvements in Active Directory deliver key strategic benefits for small, medium and large enterprises. Expanding upon the foundation established in Windows 2000, Windows .NET Server 2003 improves the versatility, manageability, and dependability of Active Directory. With Windows .NET Server 2003, organizations can benefit from further reductions in cost while increasing the efficiency with which they share and manage the various elements of the enterprise.

Benefit	Description
Greater Flexibility	Active Directory introduces important new features ensuring that it is one of the most flexible directory structures in the marketplace today. As directory enabled applications become more prevalent, organizations can utilize the capabilities of Active Directory to manage even the most complicated enterprise network environments. From Internet data centers to large distributed branch office enterprises, the improvements provided by Windows.NET Server simplify administration and increase performance and efficiency, making it a truly versatile solution.
Reduced Total Cost of Ownership	Active Directory has been enhanced to reduce total cost of ownership (TCO) and operation within the enterprise. New features and enhancements have been incorporated at all levels to extend versatility, simplify management, and increase dependability. Active Directory's capabilities have also been enhanced to support your customers and partners through deployment as an extranet or Internet directory, in addition to managing Windows-based users. Deploying Active Directory in these new roles further reduces your TCO by allowing you to standardize on one directory technology for all roles.

Features and Improvements

Windows .NET Server 2003 will bring many improvements to Active Directory, making it even more versatile, dependable, and economical to use.

Feature	Description
Cross-Forest Trust and Management	Users can securely access resources in other forests without sacrificing the single sign-on and administrative benefits of having only one user ID and password maintained in the user's home forest. Additional security features make it easier to manage the multiple forests and cross domain trusts. A new credential manager provides a secure store of user credentials and X.509 certificates. In addition, Forest trust provides a new type of Windows trust for managing the security relationship between two forests—greatly simplifying cross-forest security administration and authentication.
Domain Rename	This feature supports changing the Domain Name System (DNS) and/or NetBIOS names of existing domains in a forest such that the resulting forest is still "well formed." This feature is particularly useful in scenarios where a corporation must change the names of domains. For example, when a corporation undergoes a legal name change, or when companies merge and want to have a consistent nomenclature. Using Domain Rename is much more efficient than traditional methods that may involve creating a new domain and migrating all the user and computer objects to the new domain. The identity of a renamed domain represented by its domain Globally Unique ID (GUID) and its domain Security ID (SID) will not change. In addition, a computer's domain membership does not change as a result of the holding domain being renamed. Although this feature provides a supported means to rename a domain, it is not viewed nor meant to be a routine IT operation. Domain Rename will cause a service interruption requiring every Domain Controller to be rebooted. Domain rename will also require that every member computer of the renamed domain must be rebooted twice.
Deactivation of Attributes and Class Definitions in the Schema	Active Directory's flexibility has been enhanced to allow the deactivation of attributes and class definitions in the Active Directory schema, such that attributes and classes can be redefined if an error was made in the original definition. Deactivation is a reversible operation, so it will be possible to undo an accidental deactivation without side-affects. For example, if a new schema object is added to the directory incorrectly, an administrator can use this feature to deactivate the object and re-enter the correct definition for the object. A Windows 2000 Domain Controller cannot be upgraded to a later server version if a new schema object introduced in the Active Directory schema in the later version conflicts with a user-introduced schema extension. An IT administrator can use the schema deactivate feature to move the offending schema object out of the way in order to allow the system upgrade to proceed. This feature also allows developers more flexibility in developing to the Active Directory. If, for example, a developer includes attributes and classes as Active Directory schema extensions during development of a new application and later finds a need to change the definition of an attribute, this feature allows the developer to make such a change while preserving the identity of the attribute. Or if a business group has replaced use of several applications that extended the Active Directory schema with a new application that uses the Active Directory schema. This feature provides the IT administrators the ability to deactivate the unused schema objects of the applications that are replaced so that they do not conflict with any new

	extensions that may be installed.
Support for the inetOrgPerson Class	An IT administrator can use this feature to migrate their inetOrgPerson objects from an LDAP directory to Active Directory, to compare information in Active Directory to other LDAP directories or to create inetOrgPerson objects in Active Directory. ISVs can easily port applications that are based on the inetOrgPerson class to Active Directory. Active Directory supports definition of user objects based on the inetOrgPerson class as defined in RFC 2798. This feature includes supporting attributes to the base schema for these user objects. The User Interface (UI) that works with user objects also supports inetOrgPerson objects. Ancillary features include user password defined at user creation time, a samAccountName automatically generated if one is not provided, and the userPassword attribute can be used to set the account password using standard text.
Install Replica from Media	Instead of replicating a complete copy of the Active Directory database over the network, this feature allows an administrator to source initial replication from files created when backing up an existing DC or Global Catalog server. This feature is particularly useful when bandwidth is at a premium. For example, a company might want to place a replica DC in a remote site that has low bandwidth network connectivity. Replicating the entire directory over this link can be time consuming. The backup files, generated by any Active Directory-aware backup utility, can be transported to the candidate DC using media such as tape, Compact Disk (CD), Digital Video Disc (DVD), or file copy over a network. In order to use this feature, you must run the Active Directory Installation Wizard in Advanced Mode (dcpromo.exe/adv).
Improved Replication of Group Membership	As group members are added, changed or deleted only those changes are replicated resulting in lower network bandwidth and processor usage during replication and virtual elimination of the possibility of lost updates during simultaneous updates. In Windows 2000 Active Directory, the membership of a group is stored and replicated as a single unit. As a result, a change to a group with large membership caused the entire membership to replicate, consuming a less-than-optimal amount of network bandwidth and increasing processor load. In addition, if the membership of a group is updated simultaneously on two or more Windows 2000 domain controllers, then some of the membership updates could theoretically be lost during replication conflict resolution. When a forest is advanced to Forest Native Mode of Windows .NET Server 2003 Family, group membership is changed to store and replicate values for individual members instead of treating the entire membership as a single unit. When an IT administrator makes updates to security groups or mail distribution lists to a Domain Controller running in Forest Native Mode of Windows .NET Server 2003 Family, integrity of the updates are maintained.
Easier Logon for Remote Offices	The loss of connectivity between a branch office and a global catalog no longer impacts the ability of branch users to logon. Branch offices with domain controllers can provide user logon through cached credentials without first contacting the Global Catalog, improving system performance and robustness over unreliable wide area networks. In Windows 2000, when processing a logon for a user in a native mode domain, a Domain Controller (DC) had to contact a Global Catalog (GC) server in order to expand a user's Universal Group membership. This requirement compelled some organizations to deploy GC servers into remote offices in order to avoid logon failures if the network

	link that connected the remote site to the rest of the organization was disconnected. In Windows .NET Server 2003, DCs in a site that does not contain a GC server can be configured, through the Active Directory Sites and Services Snap-in, to cache Universal Group membership lookups when processing user logons. This allows a DC to process logons without contacting a GC and when a GC server is unavailable. Group memberships for users that log on to the DC in the site will be cached. The cache will be refreshed on a periodic basis as determined by the replication schedule. This also results in reduced bandwidth requirements for replication.
Improved Performance Features	Windows .NET Server 2003 more efficiently manages the replication and synchronization of Active Directory information. Administrators can better control the types of information that are replicated and synchronized between domain controllers both within a domain as well as across domains. In addition, Active Directory provides more features to intelligently select only changed information for replication—no longer requiring updating entire portions of the directory.
Improved Synchronization Features	This feature allows a company to scale their enterprise more effectively. When the Global Catalog's Partial Attribute Set (PAS) is extended, such as for a line-of-business application deployment or any administrative action, new capabilities will minimize the impact to the administrator's network infrastructure. This is especially important for administrators with large directories and those with global networks that include slower speed links. With Windows 2000, the Global Catalog (GC) Partial Attribute Set requires that, upon propagation of extended PAS (addition of an attribute to the PAS), the GC initiates a full synchronization cycle of its Read-Only (RO) Naming Context (NC). This is done to become up-to-date with the attribute-extended replica image on other Domain Controllers (DC). This feature provides a mechanism to preserve the GC synchronization state (rather than re-setting it) and minimizes the work and data replicated when an extended PAS is propagated across the enterprise
Increased Dependability	Active Directory includes several new features that increase dependability such as Health Monitoring, which allows administrators to verify replications between domain controllers, improved Global Catalog replication, and an updated Inter-Site Topology Generator (ISTG) that scales better by supporting forests with a greater number of sites than Windows 2000. In Windows 2000, the process that automatically created replication connections between Domain Controllers in different sites could not be used when a forest contained a large number of sites. Instead, administrators had to create and maintain manual inter-site replication topologies. In Windows .NET Server 2003, the Inter-Site Topology Generator (ISTG) has been updated to use improved algorithms and will scale to support forests with a greater number of sites than in Windows 2000. Because all Domain Controllers in the forest running the ISTG role must agree on the inter-site replication topology, the new algorithms are not activated until the forest has advanced to Active Directory forest functionality level of Windows .NET Server 2003 Family (described in the feature Active Directory: Forest and Domain Functional Levels). After an IT administrator advances the forest to Server Active Directory forest functionality level of Windows .NET Server 2003 Family, Active Directory will automatically use the improved ISTG to generate the inter-site replication topology.

Disabling Compression of Replication Between Sites	When a number of sites are connected with a high-speed network where bandwidth is not at a premium you can selectively disable compression of replication between Domain Controllers residing in different sites. This results in a reduction of the Central Processing Unit (CPU) utilization on the Domain Controllers and increased availability.
Forest and Domain Functional Levels	There are certain features in Active Directory, such as Group Membership Replication Improvements and Inter-site Replication Topology Generator, that cannot be activated until the Domain Controllers (DCs) in a forest are upgraded to the Windows .NET Server 2003 Family. Forest and Domain Functional Levels is a feature which provides a versioning mechanism that can be used by Active Directory core components to determine what features are available in a forest or domain. It is also used to prevent computers running pre-Windows .NET Server 2003 Family operating system Domain Controllers (DCs) from joining a forest or domain that has Active Directory features activated that only apply to the Windows .NET Server 2003 Family operating system. In order to take advantage of the advanced functionality of Windows .NET Server 2003 domains features, an IT administrator can advance the forest or domain functional level to Windows .NET Server 2003 Family after all of the DCs in the forest or domain have been upgraded to run the Windows .NET Server 2003 Family operating system. This feature is accessed from the NTDSUTIL utility.
Forest and Domain Upgrade with ADPrep	Active Directory has added improvements regarding security and application support. Before the first Domain Controller running the Windows .NET Server 2003 operating system can be upgraded in an existing forest or domain, the forest and domains have to be prepared for these new features. ADPrep is a new tool to aid forest and domain upgrades. The ADPrep tool is not needed when upgrading from Windows NT 4 or when a clean installation of Active Directory is made on servers running the Windows .NET Server 2003 Family operating system. To prepare the forest, the administrator has to run <code>adprep /forestprep</code> on the schema operations master. To prepare a domain, the administrator has to run <code>adprep /domainprep</code> on the infrastructure operations master in each domain.
Lightweight Directory Access Protocol	The Lightweight Directory Access Protocol (LDAP), an industry standard, is the primary access protocol for Active Directory. LDAP version 3 was defined by the Internet Engineering Task Force (IETF). Microsoft is committed to incorporating changes to this standard within Active Directory. Administrators, application developers and 3rd party ISVs benefit by being able to take advantage of the latest advances to the LDAP standard. Windows .NET Server 2003 Family includes several enhancements to the Lightweight Directory Access Protocol (LDAP) client and server implementation: • Support for Dynamic Entries: Active Directory can store dynamic entries according to the Internet Engineering Task Force (IETF) standard protocol RFC 2589. Entries in the directory can be assigned Time-To-Live (TTL) values that determine when the entries will be automatically deleted. • Transport Layer Security (TLS) support: Connections to Active Directory over LDAP can now be protected using the IETF standard TLS security protocol, as specified in RFC 2830. • Support for the Digest Authentication mechanism. Connections to Active Directory over LDAP can now be authenticated using the DIGEST-MD5 SASL authentication mechanism as specified in RFC 2829. • Virtual List Views (VLV): When an LDAP query has a large result set, it is

	inefficient for a client application to pull down the entire result set from the server. VLV allow a client application to “window” through a large result set without having to transfer the entire set from the server. The VLV protocol was defined by the LDAP extensions Working Group of IETF. • Support for Dynamic Auxiliary classes: Active Directory now supports dynamically associating an auxiliary class (which adds the attributes that are defined by the auxiliary class) with individual object instances. In Windows 2000, an auxiliary class could only be statically associated with a structural class definition in the schema, which meant that all instances of that structural class got the attributes from the auxiliary class added to them. • Support for “fast bind” and connection re-use: At the request of numerous ISVs and application developers we have enhanced Active Directory to support fast binds and connection re-use. Many web applications use Active Directory as an authentication store. Fast binds allow a web, or any other application, to request simple authentication verification from Active Directory without generating Windows-specific authorization information resulting in increased performance of these applications. An application may also re-use an initial connection to the directory for multiple queries on behalf of different users. This also results in increase performance since the application does not have to re-establish a connection for each query. These enhancements are of particular importance to web applications that are servicing tremendous numbers of Internet-based queries.
Metadirectory Support	Microsoft Metadirectory Services (MMS) helps companies to integrate identity information from multiple directories, databases and files with Active Directory. MMS provides an organization with a unified view of identity information, enables the integration of business processes with MMS and helps to synchronize identity information across an organization.
DirSync Control Improvements	Windows 2000 Active Directory supports a Lightweight Directory Access Protocol (LDAP) control, called DirSync control, to retrieve changed information from the directory. This feature provides a method to imbue the DirSync control with the ability to perform access checks like those performed on normal LDAP searches.
WMI Providers for Replication and Trust Monitoring	Monitoring of trusts and Active Directory replication is made easier through the use of Windows Management Instrumentation (WMI). This feature provides WMI classes to monitor whether Domain Controllers are successfully replicating Active Directory information among themselves. Because many Windows 2000 components, such as Active Directory replication, rely on inter-domain trust, this feature also provides a method to monitor that trusts are functioning correctly. IT administrators or independent software developers can also use this feature to write scripts or applications that monitor the health of Active Directory replication and inter-domain trust.
Application Directory Partitions	Some directory information does not need to be made globally available. This feature provides the capability to host data in Active Directory without significantly impacting network performance by providing control over the scope of replication and placement of replicas. Active Directory services will allow the creation of a new type of Naming Context (NC), or partition, referred to as Application Partition. This NC can contain a hierarchy of any type of objects except security principals (users, groups and computers), and can be configured to replicate to any set of Domain Controllers in the forest, not necessarily all

	in the same domain. This means that dynamic data from network services such as Remote Access Service (RAS), RADIUS, Dynamic Host Configuration Protocol (DHCP) and Common Open Policy Service (COPS) can reside in a directory so that applications can access them uniformly with one access methodology. Developers will be able to use this feature to write applications data to dedicated application directory partitions rather than to a domain partition.
Lingering Objects Removal Mechanism	This feature prevents inconsistency between various replicas of the Active Directory that may lead to security issues and reduces growth of the Active Directory database size. Lingering objects may exist in the Active Directory due to a long unavailability of a Domain Controller during which the tombstone life time of the objects has expired and the tombstone objects were removed from the Active Directory. This feature provides the ability to delete lingering objects in the Active Directory.
Prevent Overloading Domain Clusters	This feature prevents overloading a first Active Directory Domain Controller introduced in a domain that already contains a large number of upgraded domain members running Windows 2000 and Windows .NET Server 2003 Family. This feature is useful when a Windows NT4 domain contains domain members running Windows 2000, Windows XP Professional and Windows .NET Server 2003 Family. When a Primary Domain Controller (PDC) is upgraded to Windows 2000 Service Pack 2 or Windows .NET Server 2003 Family it can be configured to emulate the Windows NT4 DC behavior. The domain members running Windows 2000 and Windows .NET Server 2003 Family will not distinguish upgraded DCs from Windows NT4 DCs. To accommodate special needs of IT administrators, the domain members running Windows 2000 Service Pack 2 and Windows .NET Server 2003 Family can be configured to inform a DC running Windows 2000 Service Pack 2 and Windows .NET Server 2003 Family to not emulate Windows NT4 DC behavior when responding to such domain members. This configuration is performed through the Registry Editor.
Remove non-X500 compliant RDN Restrictions	In Active Directory, the naming attribute (also known as the Relative Distinguished Name, RDN, attribute) is defined in the schema for each class. For example, the user class uses the Common Name (CN) as the naming attribute. Classes that do not define a naming attribute inherit the naming attribute from their parent class. After a naming attribute is selected, it cannot be changed. Active Directory also has the requirement that RDNs must be unique within a container, resulting in the inability to have two users with the same RDN to be in the same container. This feature has been enhanced in the Windows .NET Server Family to allow the ability to delete inetOrgPerson (which uses CN as the naming attribute in the default schema) and re-create it using any Unicode string attribute as the naming attribute. Instead of CN, any other attribute can be used as the naming attribute. If, for example, there are several users in the Same OU that have the same name, this feature would enable the administrator to choose an identifying attribute for the users that will guarantee that there are no naming collisions. This is also useful in a situation where directories are being merged, as in a corporate acquisition. If a company has acquired another business that is running another Lightweight Directory Access Protocol (LDAP) directory that uses a different naming attribute for their inetOrgPerson objects, the administrator can use this feature to modify the naming attribute and then migrate the inetOrgPerson objects from the LDAP directory to Active Directory.

Improved Management and User Interface

Windows .NET Server 2003 introduces enhancements to several Active Directory management interfaces. Administrators may now edit multiple user objects simultaneously, reset ACL permissions to the default, show effective permissions on a security principal and indicate the parent of an inherited permission.

Feature	Description
Improved Installation and Configuration	This feature simplifies debugging, handling and reporting of an incorrect Domain Name System (DNS) configuration and helps to properly configure the DNS infrastructure required for Active Directory deployment. This includes the following: • If a Domain Controller (DC) is promoted in an existing forest, the Active Directory Installation Wizard contacts an existing DC to update the directory and replicate from the DC the required portions of the directory. If the Wizard fails to locate a DC due to an incorrect configuration of DNS or if the DC is not available, it performs debugging and reports what caused the failure and how to fix the problem. • In order to be located on a network, every DC must register in DNS DC locator DNS records. The Active Directory Installation Wizard verifies that DNS infrastructure is properly configured to allow new DC to perform dynamic update of its DC locator DNS records. If this check discovers the incorrectly configured DNS infrastructure, it is reported with an explanation on how to fix the problem. If the DNS infrastructure is properly configured to allow Active Directory deployment, the IT administrator will not notice a presence of this feature. Otherwise, if the DNS infrastructure is incorrectly configured and prevents Active Directory deployment, it will be brought to the IT administrator's attention when they attempt to perform Active Directory installation using Active Directory Installation Wizard.
Active Directory Migration Tool	It is now easier to migrate to Active Directory through a number of improvements that have been made to the Active Directory Migration Tool (ADMT). ADMT version 2 now allows migrating passwords from Windows NT 4 to Windows 2000 and Windows .NET Server 2003 Family or from Windows 2000 and Windows .NET Server 2003 Family to Windows 2000 and Windows .NET Server 2003 Family domains. For the most commonly used migration tasks, such as migration of users, groups and computers, a new scripting interface was added. ADMT can now be driven from any language and supports COM interfaces, such as Visual Basic® Script, Visual Basic and Visual C++® development systems. The scripting interface has also been extended to provide command line support. All scriptable tasks can be executed directly from a command line or through batch files. These scripting and COM interface improvements make it easier for developers to integrate ADMT into their applications and enables ADMT to be used batch only scenarios.
Enhanced User Interface	As the principal means to manage enterprise identities, objects, and relationships, the Microsoft Management Console (MMC) plug-ins now includes drag-and-drop capabilities, multi-object selection, and the ability to save and reuse queries.
Improvements to the Object Picker	Administration of Active Directory has been made easier through improvements made to the object picker User Interface (UI) and other administrative UIs that allow an administrator to select one or more users, computers, groups, or contacts. The object picker is used by numerous UIs and is available for use by third-party

	developers. To that end, it provides public and private interfaces that the launcher can use to customize the behavior to their needs. For example, it can be launched in single-select mode or in multi-select mode or it can be launched to allow only one specific type of object (such as Users) to be selected. The Object Picker has been redesigned and enhanced, with the following results: • Optimized administrator workflow allows very quick finding of directory objects • Improved support for finding objects in a large directory • Directory Service impact on a network is reduced • Ability to scope a search down to a specific Organizational Unit (OU) within the directory • More flexible querying capabilities for finding objects in the directory based upon their attributes
Active Directory Users and Computers: Saved Queries	This feature will allow queries to be saved, reopened, refreshed and e-mailed making administration easier. A query is a search against a data set (the directory) for items that match particular criteria (such as directory object attribute values). Query objects and results can be viewed and manipulated in the User Interface. This feature has a number of benefits for administrators: • An IT administrator can use this feature to export the results of an attribute query for reporting or analysis. They can refresh the query on a periodic basis and thus save time in completing management reports. • An IT administrator can use this feature to select a set of users based on their attribute properties and then add them en masse to a group. • An IT administrator can query the directory to find a particular set of user objects, then edit the properties on all of them at once (as described in the feature "Active Directory: Editing of Multiple User Objects"). • An IT administrator can use this feature to identify all of the accounts that are disabled, identify all of the accounts that expire on a specific date, identify all user accounts with non-expiring passwords, identify all system accounts with RAS-enabled, find user accounts with passwords older than a specific number of days, find accounts with RAS callback enabled, and find all accounts without managers. • An IT administrator can query the directory to find a particular set of user objects, then edit the properties on all of them at once, as described in the new feature "Active Directory Users and Computers Snap-in: Simultaneous Editing of Multiple User Objects."
Active Directory Users and Computers: Editing Multiple User Objects	This feature provides the capability to select multiple user objects, and then bring up a set of property sheets that will allow the clearing or setting of object attributes across all the selected objects. Only specific property sheet and attributes will be available for this multi-object editing. This feature can be used to change attributes for a large number of objects simultaneously with only a few steps making administration easier.

Improvements and New Features in Group Policy

Group Policy allows you to define the settings and allowed actions for users and computers. In contrast with local policy, you can use Group Policy to set policies that apply across a given site, domain, or organizational unit in Active Directory. Policy-based management simplifies such tasks as

system update operation, application installation, user profiles, and desktop-system lockdown. Over 100 new policy objects have been added to the directory for Windows .NET Server 2003.

Feature	Description
Resultant Set of Policy (RSoP)	This tool allows an IT administrator to determine the resulting set of policy for a given user or computer in both an actual and a what-if scenario. The logging mode allows an IT administrator to examine what was actually processed on a given computer. The planning mode allows an IT administrator to perform “what if” analysis for a specified location in the directory, security group membership and WMI filtering properties. The Resultant Set of Policy (RSoP) wizard guides an administrator through the steps necessary to create an appropriate target, generate RSoP data, and start the RSoP tool to use that data. This tool can determine the state of an existing target and run scenarios by manipulating the way in which Group Policy might be applied. It allows access and inspection of RSoP for a given target, allows generation and inspection of RSoP for a given target in an artificial environment, and allows easy inspection of differences under new criteria. Resultant Set of Policy is available through the Active Directory Users and Computers MMC snap-in or through the Resultant Set of Policy MMC snap-in.
Group Policy: New Policies	These policies provide improved capability to manage, customize and control the behavior of the Operating System for groups of users. Over 160 new policy settings are now available in the operating system. These new policy settings affect functionality such as Control Panel, error reporting, Terminal Services, Remote Assistance, networking and dial-up connections, Domain Name System (DNS), network logon, Group Policy and roaming profiles. • Netlogon: Netlogon policies provide the capability to configure the Netlogon settings on computers running Windows .NET Server 2003 Family using Group Policy. This simplifies the steps required to configure domain members when adjusting Netlogon settings such as enabling and disabling dynamic registration of the specific Domain Controller (DC) locator Domain Name System (DNS) records by the DCs, periodicity of refreshing such records, enabling and disabling auto-site-coverage and many other popular Netlogon parameters. • Credentials Manager: Credential Manager is provided to make use and management of user credentials. This Group Policy feature provides the ability to allow Credential Manager to be disabled. • 64-bit Software: 64-bit software policy provides support for 64-bit software deployment with Group Policy. New options in the Application Deployment Editor (ADE) aid in determining if 32-bit applications should be deployed to 64-bit clients. The ADE also allows existing Windows 2000 deployments to be managed with the same level of functionality provided by Windows XP or Windows .NET Server 2003 Family. • Support URL: This feature provides a capability to edit and add a support Uniform Resource Locator (URL) for the package. When the application appears in the Add/Remove Programs on target computers, the user can then select the Support Information URL and will be directed to a support Web page. This feature can assist in reducing calls to a helpdesk or support team. • Terminal Services: Terminal Services policies now provide Group Policy settings for most configurations. My Documents: Through Group Policy, this feature provides the capability to redirect a

	user's My Documents folder to their home directory.
Manage DNS Using Group Policy	This feature allows administrators to easily manage and configure the Domain Name System (DNS) client settings on computers running Windows .NET Server 2003 Family operating system using Group Policy. This simplifies the steps required to configure domain members when adjusting DNS client settings such as enabling and disabling dynamic registration of the DNS records by the clients, using devolution of the primary DNS suffix during name resolution and populating DNS suffix search lists. In addition to the simplification of the administration, Group Policy support for the last parameter (DNS suffix search list) is considered a strategic feature, which will be required in a transition to the NetBIOS-less environment.
Software Restriction Policies	This allows you to improve management of computers running Windows XP and Windows .NET Server 2003 Family in a way that allows better defenses against viruses, Trojans and unwanted applications. Software Restriction Policies provides a policy-driven mechanism to identify software running in a domain and control its ability to execute. It can identify software that is hostile or unwanted and prevent it from executing on computers running Windows XP and the Windows .NET Server 2003 Family. This feature also allows you to limit the software that runs on highly managed workstations (such as kiosks, task stations, or application stations) to only a certain list of software. This can help improve system stability and integrity for these computers. This feature is run from the Manage Group Policy snap-in.
Administrative Templates Web View	This feature enhances the Group Policy Administrative Template extension snap-in making it possible to view detailed information about the different available policy settings. When a policy setting is selected, information detailing the settings behavior and additional information on where the setting may be used is displayed in a Web View within the Administrative templates UI. This information is also available from the Explain tab on the Property page of each setting.
WMI Filtering	The Windows Management Instrumentation (WMI) Filtering is an addition to the Group Policy infrastructure to enable the ability to specify a WMI-based query to filter the affect of a Group Policy Object (GPO). This will be an addition to the GPO Properties page as a new tab where a filter can be specified, created and edited. Additionally, support is included to allow Resultant Set of Policies (RSOP) to display existing WMI filters as well as specify alternate WMI filters. This is similar in concept to the Security Group filtering that was implemented in Windows 2000.
Group Policy Management Console	Expected to be freely available on the Microsoft Web site shortly after the release of Windows .NET Server 2003, the Group Policy Management Console (GPMC) will provide the new framework for managing Group Policy. With GPMC, Group Policy becomes much easier to use, a benefit that will enable more organizations to better utilize the Active Directory service and take advantage of its powerful cost saving features. For example, GPMC enables backup and restore of Group Policy objects (GPOs), import/export and copy/paste of GPOs, reporting of GPO settings and Resultant Set of Policy (RSOP) data, and scriptability for all GPMC operations. For example, with import and copy paste of GPOs, administrators can maintain pre-built versions of GPOs for various configurations (highly managed desktops, laptops, Terminal Services on Windows .NET Server 2003, Exchange Servers, etc) and rapidly deploy them throughout their organization as needed. In addition, GPMC lets administrators manage Group Policy for multiple domains and

	sites within a given forest, all in a simplified user interface (UI) with drag-and-drop support. And with cross-forest trust, administrators can manage Group Policy across multiple forests from the same console. GPMC can manage Group Policy for Windows 2000 or Windows .NET domains.
Cross-Forest Support	The cross-forest feature in Windows.NET Server enables several new scenarios that Group Policy supports. While Group Policy Objects can only be linked to sites, domains, or OUs within a given forest, Windows.NET Group Policy successfully supports these new interoperability scenarios For example, it is possible for a user in forest A to log on to a computer in forest B, each with their own sets of policy. Alternatively, settings within a GPO can reference servers in external forests, for example software distribution points.
Software Restriction Policies	This feature provides a policy-driven mechanism to identify software running in a domain and control its ability to execute. It can identify software that is hostile or unwanted and prevent it from executing on computers running Windows XP and the Windows .NET Server 2003 Family. This allows you to improve management of computers running Windows XP and Windows .NET Server 2003 Family in a way that allows better defenses against viruses, Trojans and unwanted applications. This feature also allows you to limit the software that runs on highly managed workstations (such as kiosks, task stations, or application stations) to only a certain list of software. This can help improve system stability and integrity for these computers. This feature is available from the Group Policy Object Editor snap-in.
Enhanced User Interface in the Group Policy Object Editor	Policy settings are more easily understood, managed, and verified with Web-view integration in the Group Policy Object Editor. Clicking on a policy instantly shows the text explaining its function and supported environments such as Windows XP only or Windows 2000.
WMI Filtering	Windows Management Instrumentation (WMI) Filtering enables administrator to determine whether to apply a Group Policy Object (GPO) to a specific computer or user based on WMI properties of the target computer/user. This is similar in concept to the Security Group filtering that was implemented in Windows 2000.
Folder Redirection Enhancements	Administrators can now choose to redirect users' My Documents folder to the user's home directory.
Enhancements to Group Policy-based Software Distribution	Microsoft has implemented the following enhancements in .NET Server. Administrators can now choose to assign applications to users and have them either fully installed at logon, or on demand when the user starts the application. The option for this support is in the Software Settings node of the Group Policy Object Editor. Administrators can now specify a URL that will appear in the user's Add or Remove Programs applet that will point to support information.

Summary

Building on Windows 2000, Active Directory in Windows .NET Server 2003 emphasizes simplified management, versatility, and unmatched dependability. More than ever, Active Directory has become a solid foundation for building enterprise networks unsurpassed in its ability to:

- Take advantage of existing investments and consolidation management of directories.

- Extend administrative control and reduce redundant management tasks.
- Simplify remote integration and use network resources more efficiently.
- Reduce TCO and improve the utilization of IT resources.

More Information

Microsoft will publish a longer detailed technical overview of this Windows .NET Server 2003 technology on the Web when Release Candidate 1 of Windows .NET Server 2003 becomes available.

Link to these longer technical articles at

<http://www.microsoft.com/windows.netserver/techinfo/overview> .

Application Services

Introduction

Windows .NET Server 2003 builds on the core strengths of the Windows family of operating systems—security, manageability, reliability, availability, and scalability. Advances in Windows .NET Server 2003 will provide many benefits for developing applications, resulting in lower total cost of ownership (TCO) and better performance. This section provides an overview of benefits, new features, and improvements for application services in Windows .NET Server 2003.

Benefits

The Windows .NET Server 2003 application environment provides the following benefits.

Benefit	Description
Simplified Integration and Interoperability	Easily connect with partners and customers, protect and extend existing infrastructure, and build dynamic applications.
Improved Developer Productivity	Get products to market faster, develop applications that are on time and on budget, and take advantage of quicker and easier build cycles.
Increased Enterprise Efficiency	Meet customer demands while keeping costs down, improve productivity by using fewer people with better results, and build high-performance applications.

New Features and Improvements

Windows .NET Server 2003 provides the following:

- Simplified Integration and Interoperability.
- Improved Developer Productivity.
- Increased Enterprise Efficiency.
- Improved Scalability and Reliability.
- End-to-End Security.
- Efficient Deployment and Management.

Simplified Integration and Interoperability

As the foundation of the .NET platform, Windows .NET Server 2003 will deliver a revolutionary application environment to build, deploy, and run XML Web services. Integrating support for XML Web services enables applications to take advantage of the loosely coupled principles of Internet computing.

Feature	Description
Native XML Web Services Support	Windows .NET Server 2003 offers native support for XML Web service standards including XML, SOAP, UDDI, and Web Services Description Language (WSDL).

Enterprise UDDI	Windows .NET Server 2003 ships with an enterprise version of the UDDI service. This means companies can run their own internal UDDI server, allowing developers in an organization to easily and quickly find the Web services available within the organization.
Support for Existing Services	Because XML Web services are deeply integrated into Windows .NET Server 2003, existing services like COM+ and MSMQ (Microsoft Message Queuing) can readily take advantage of them. Administrators can allow existing COM+ applications to be called using XML/SOAP by simply checking a configuration box.
Federation Infrastructure	Federation infrastructure is fundamentally about enabling servers and services to interoperate across trust boundaries.

Improved Developer Productivity

The Windows .NET Server 2003 application environment improves the productivity of developers by providing a complete set of integrated application services and industry-leading tool support.

Feature	Description
Microsoft .NET Framework	The .NET Framework is the infrastructure for the overall .NET platform. The Framework incorporates the common language runtime (CLR) and a unified set of class libraries that include Windows Forms, ADO.NET, ASP.NET, and other capabilities. The .NET Framework provides a fully managed, protected, and feature-rich application execution environment, simplified development and deployment, and seamless integration with a wide variety of programming languages. By integrating the .NET Framework into the Windows .NET Server 2003 application development environment, developers are freed from writing "plumbing" code and can instead focus their efforts on delivering real business value. The Framework—which Windows 2000, Windows 95, Windows 98, Windows Me, and Windows NT 4.0 all support—enables developers to create great Web applications with the help of ASP.NET and other technologies. It can also help them build the same applications they design and develop today. The .NET Framework provides deep, cross-programming language integration that boosts productivity by enabling developers to extend one programming language's components within another language by way of cross-language inheritance, debugging, and error-handling. Windows .NET Server 2003 provides the richest set of services available with any development platform, including comprehensive data access, integrated security, interactive user interfaces, mature component object model, transaction processing monitors, and world-class queuing.
ASP.NET: Simple Web Service Creation	This feature provides the ability to create an application without the need to add service infrastructure code to the application. This is accomplished using ASP.NET Web service features. An application developer can use ASP.NET features to write business logic and the ASP.NET infrastructure will be responsible for delivering the service by using Simple Object Access Protocol (SOAP) and other public protocols.
Separate Code from Content	The .NET Framework enables developers and content creators to work in parallel by keeping content separate from application code.

Industry-leading Tools	Microsoft Visual Studio® .NET provides an integrated, multilanguage tool for building Web applications and XML Web services.
Reusable Code	ASP.NET provides an intelligent architecture that is easy to learn and that allows for improved code reuse.
Server-side Web Controls	The new ASP.NET functionality increases productivity by encapsulating complex interactions in server-side components. Developers can rapidly build scalable Web applications that can service multiple-user interface devices. Web controls are compiled and run on the server for maximum performance, and can be inherited and extended for even more functionality.
Component Services	Component Services is a set of services based on extensions of the Component Object Model (COM) and on Microsoft Transaction Server (an earlier release of a component-based transaction processing system). Component Services provides threading and security, transaction management, object pooling, queued components, and application administration and packaging.
Message Queuing	The Message Queuing feature helps developers build and deploy applications that run more reliably over networks, including the Internet. These applications can interoperate with applications running on different platforms, such as mainframe computers and UNIX-based systems.
Application Verifier	The Application Verifier tool provides functionality enabling applications that run on the operating system to be tested and verified. This tool focuses on subtle issues such as heap corruptions and compatibility issues.
New Developer APIs	Windows .NET Server 2003 introduces a number of new Application Programming Interfaces (APIs), making it a more efficient and flexible development platform. These new APIs include: Managing IP Security: Windows .NET Server 2003 includes a local system management API to control Internet Protocol (IP) Security (IPSec). User Token API: The new user token Application Programming Interface (API) is provided to enable a method to get the user's token. This is commonly needed for cross session communications when an application needs to perform an action in the user's security context.

Increased Enterprise Efficiency

Applications developed in the Windows .NET Server 2003 environment are more responsive and available, and because the environment can be managed by fewer people, it will deliver lower TCO with better performance, improved scalability and reliability, and more robust security. In addition, Windows .NET Server 2003 eases the burden on IT administrators, by making it easier to deploy and manage applications.

Feature	Description
ASP.NET: Session Monitoring	This feature increases reliability by monitoring running ASP.NET applications. The feature will also stop and start applications when necessary.
Automatic Memory Management	The .NET Framework runs in the Common Language Runtime, which is a garbage-collected environment. Garbage collection frees applications that are using .NET

	Framework objects from the need to explicitly destroy those objects, reducing common programming errors dramatically such as heap fragmentation issues by using a classic allocation/free model.
Enterprise UDDI Services	UDDI Services is the Web Services infrastructure in Windows .NET Server 2003 that helps companies organize and catalog programmatic resources and provides an efficient mechanism for discovery, sharing and reuse of Web Services.
COM+ 1.x Enhancements	Windows .NET Server 2003 includes several enhancements to the Component Object Model (COM), including: Applications as Services: This enhancement of Common Object Model+1.x (COM+ 1.x) enables you to configure a COM+ server application as a service and implement the service as a COM+ server application. This provides more control over COM+ application startup. Marking the application to run as a service means that the component's Dynamic Link Library (DLL) is loaded into memory when the system boots. This results in making a COM+ application highly available and enables it to be installed on a clustered server. Application Partitions: Application Partitions allow multiple versions of COM+ applications to be installed and configured on the same computer. This results in more cost-effective management of server applications. Application Process Dump: Pause/Disable Applications provides a new process dump of the entire state of a process without terminating that process. Component Aliasing: COM+ 1.x provides component aliasing. This allows the ability to configure one physical implementation of a component multiple times. Configurable Isolation Levels: COM+ 1.x provides the ability to configure isolation levels much more flexibly than was previously possible. Low Memory Activation Gates: COM+ 1.x prevents situations in which error paths might be run on a server. Rather than waiting for memory allocations to fail in a section of code, COM+ checks memory before it creates a COM+ server or object. If the percentage of virtual memory available to the application falls below a fixed threshold, the activation fails before the object is created. Process Recycling: This enhancement enables you to configure process recycling administratively through the COM+ User Interface (UI), or programmatically through the COM+ administrative Software Development Kit (SDK). Processes can be shut down or recycled based on several criteria, including elapsed time, memory usage, number of calls, and the number of activations. Public/Private Components: This feature allows you to mark components as private components that can only be seen and activated by other components in the same application. Private components can also be marked to block access from outside the application (while still taking advantage of COM+ services). This provides more control over functionality of an application.
Compatibility Mode	A new Compatibility Mode feature ensures out-of-box compatibility for many popular applications. Compatibility Mode technology provides an environment that more closely reflects the behavior of Windows 95, Windows 98, Windows NT 4.0, or Windows 2000 operating systems. These modes resolve several of the most common issues that prevent older applications from working correctly. Applications that experience problems after migration might benefit from being started in one of these compatibility environments. Advanced users can also take advantage of this technology to create solutions for their own applications. One of the compatibility technologies in Windows .NET Server 2003, called AppFixes,

	solves problems such as applications incorrectly detecting the operating system version and specific application problems such as referencing memory after it has been freed. The infrastructure support enables AppFixes without user intervention on applications that would otherwise be considered incompatible. Windows .NET Server 2003 maintains an AppFixes database that can be updated through Auto Update. AppFixes can also be activated by an end-user through the application's property page.
--	--

Improved Scalability and Reliability

Here are some of the key scalability and reliability features that benefit developers and IT professionals in an application environment.

Feature	Description
ASP.NET: Integrated with IIS 6.0	ASP.NET is integrated with the Internet Information Services (IIS) 6.0 process model and leverages support for multiple application pools. This means that individual ASP.NET applications are isolated and talk directly to the kernel-mode http listener. This leads to a reduced number of process hops and allows ASP.NET applications to leverage kernel-mode file caching. ASP.NET is integrated with IIS 6.0 process model and leverages the support for multiple application pools. This means individual ASP.NET applications are isolated and communicate directly to the kernel mode http listener. This leads to reduced number of process hops and allows ASP.NET applications to leverage kernel mode file caching.
ASP.NET: Advanced Compilation	The .NET Framework advanced compilation provides increased performance by compiling pages instead of interpreting them. It supports both pre-compiled applications and on-the-fly-compiled applications. ASP.NET leverages more advanced threading models that allow it to perform asynchronous I/O, leading to improved performance and scalability. This eliminates the need to convert server-side code before execution, and therefore conserves server resources, increasing server performance and scalability.
ASP.NET: Intelligent Caching	The ASP.NET programming model provides a cache API that enables programmers to activate caching services to improve performance. An output cache saves completely rendered pages, and fragment cache stores partial pages. Classes are provided so that applications, HTTP modules, and request handlers can store arbitrary objects in the cache as needed.
Asynchronous Support	The .NET Framework deeply integrates two asynchronous communication technologies for scalability and reliability: SOAP and Microsoft Message Queuing (MSMQ). This allows developers to build applications that are robust and can handle offline scenarios.
Web Farm Session State	The Process-Independent, Web-Farm-Compatible Session State increases reliability and scalability by storing session state in a process external to the ASP.NET application, so the state can survive application crashes and be referenced from other computers in a Web farm. ASP.NET session state is stored in a separate process and can be configured on a separate computer or persisted to a Microsoft SQL Server database.
IIS 6.0 Fault- Resilient Process Architecture	IIS 6.0 provides an architecture that delivers enhanced application isolation. Administrators can create multiple application pools and assign applications to those pools to provide isolation. Application pools can be monitored and automatically recycled to ensure application availability.

ADO.NET

ADO.NET uses a non-persistent connection and intelligent handling of state. ADO.NET actually sends XML messages between the data source and the application, opening and closing the connection as needed. The result is that applications scale much better with ADO.NET, and ADO.NET can work over many different network transports.

End-to-End Security

Security in Windows .NET Server 2003 is built on top of a single security model anchored by Active Directory. Security enhancements and innovations new to Windows .NET Server 2003 help to reduce the "attack surface" and make Windows authentication and authorization more secure and powerful by using a new application security architecture. Protocol transition capability enables any authentication on the front-end Web server to be transitioned to Kerberos in the backend.

Native integration of Microsoft Passport enables authentication and authorization for any customer or consumer, and sets the stage for future federation capabilities. When the front-end server trusts the Passport, the Passport is used for user validation and subsequent logon. Passport credentials can be mapped to the Active Directory for consumers and customers.

Efficient Deployment and Management

No-touch deployment is enabled by enhanced tools such as Windows Installer services (MSI) and by new tools such as Fusion. Fusion supports side-by-side versioning for DLLs, while its counterpart, Manifest, tells you exactly which DLLs are required. Windows Installer can contain Fusion manifests and can now describe the application that runs side-by-side, making it easier to deploy reliable applications.

Additional tools that can shorten the deployment process and ensure greater accuracy include X-copy deployment and IIS edit while running.

The Windows Management Interface (WMI) does in hours what formerly took days, using new tools in Visual Studio .NET. Reliability is improved through command-line tools that are freely available for download through the Internet. Applications and services can easily issue events and define variables.

Summary

IT professionals can take advantage of their existing IT resources to maximize productivity while minimizing TCO. Developers can extend their existing code and write new applications and Web services using their current skills. And, line-of-business managers and business decision-makers can optimize their return on investment by spending money on an operating system and gaining a world-class application development environment for the same investment.

More Information

Microsoft will publish a longer detailed technical overview of this Windows .NET Server 2003 technology on the Web when Release Candidate 1 of Windows .NET Server 2003 becomes available. Link to these longer technical articles at

<http://www.microsoft.com/windows.netserver/techinfo/overview> .

Clustering

Introduction

Clustering services have become increasingly essential for organizations deploying business-critical e-commerce and line-of-business applications.

A cluster is a group of computers that work together to run a common set of applications and provide the image of a single system to the client and application. The computers are physically connected by cables and programmatically connected by cluster software. These connections allow computers to use failover and load balancing that is not possible with a stand-alone computer.

The Windows .NET Server 2003 Family will provide two types of clustering services:

Server Clusters – Available only in Enterprise Edition and Datacenter Edition, this service provides high availability and scalability for mission-critical applications such as databases, messaging systems, and file and print services. Multiple servers (nodes) in a cluster remain in constant communication. If one of the nodes in a cluster becomes unavailable as a result of failure or maintenance, another node immediately begins providing service, a process known as failover. Users who are accessing the service continue to access the service, and are unaware that they are now being served by a different server (node). Enterprise Edition and Datacenter Edition both support 8-node clustering.

Network Load Balancing (NLB) – Available in all versions of the Windows .NET Server 2003 Family, this service load balances incoming Internet Protocol (IP) traffic across nodes in a Network Load Balancing cluster. Network Load Balancing enhances both the availability and scalability of Internet server-based programs such as Web servers, streaming media servers, and Terminal Services. By acting as the load balancing infrastructure and providing control information to management applications built on top of Windows Management Instrumentation (WMI), Network Load Balancing can seamlessly integrate into existing Web server farm infrastructures.

Benefits

Benefit	Description
High Availability	The cluster is designed to avoid a single point-of-failure. Applications can be distributed over more than one computer, achieving a degree of parallelism and failure recovery, and providing more availability.
Scalability	You can increase the cluster's computing power by adding more processors or computers.
Manageability	The cluster appears as a single-system image to end users, applications, and the network, while providing a single point-of-control to administrators locally or remotely.

New Features and Improvements

Building on the foundation established in Windows 2000, the Windows .NET Server 2003 Family provides new capabilities and features, making it easier and more efficient to deploy and manage clustering services.

Server Cluster Features

Feature	Description
Easy Setup and Configuration	The cluster service is an integral part of the Windows .NET Server 2003 operating system, and no longer an optional component. This enables a server cluster node to be configured without distribution media, and allows a server cluster to be created, or the configuration changed, using Cluster Administrator tools from a remote management station. No reboots are required to set up a server cluster configuration. Removing a node from a server cluster is as simple as evicting it from the cluster. Any cluster configuration data associated with the node is deleted automatically, and no reboots are required. When a server cluster node is being configured, the configuration process validates the hardware and software configuration to ensure that any known incompatibilities are detected prior to finalizing the configuration of the cluster service. Many configuration options are given default values to make it easier and quicker to set up a server cluster that conforms to best practices. After it is set up, a working server cluster can be customized using server cluster administrator tools. The cluster configuration infrastructure is an open interface that's available to third-party software vendors. This enables applications to seamlessly set up server cluster resources, and change their configuration during a server cluster installation. Server cluster setup is scriptable and available through command line tools, as well as the cluster administrator GUI.
Larger Clusters Now Supported	In Datacenter Server, the maximum supported cluster size has been increased from 4-nodes in Windows 2000, to 8-nodes in Windows .NET Server 2003. In Enterprise Edition, the maximum supported cluster size has been increased from 2-nodes in Windows 2000 Advanced Server to 8-nodes in Windows .NET Server 2003. By increasing the number of nodes in a server cluster, an administrator has many more options for deploying applications and providing failover policies that match business expectations and risks. Larger server clusters provide the capability to configure clusters in a wide range of topologies, such as 'N+1' configurations, where a pool of 'N' active servers is backed up by another, usually smaller, pool of '1' passive servers. Larger server clusters also be built in a multi-site, geographically dispersed configuration that provides for disaster tolerance
Integrates with Active Directory Service	Server clusters running Enterprise Edition or Datacenter Edition integrate with the Microsoft Active Directory service. This integration ensures that a "virtual" computer object is registered in Active Directory. This allows applications to use Kerberos authentication and delegation to highly available services running in a cluster. The computer object also provides a default location for Active Directory-aware services to publish service control points.
64-Bit Support	64-bit support is available in Enterprise Edition and Datacenter Edition.
Increased Manageability	When server clusters are used with storage infrastructures that allow dynamic volume growth, the cluster disks can be expanded dynamically online, with a new in-the-box tool called DiskPart.

Easy Resource Configuration	It's simpler to set up clustered printers, and the process for setting up the Microsoft Distributed Transaction Coordinator (MSDTC) is easier too—it only needs to be configured once to have configuration information replicated to all nodes. Applications can be made cluster-aware using scripting languages like Visual Basic Script and JScript®; this makes it easier to write specific resource add-ins for applications that can be monitored and controlled in a server cluster. Resource-specific properties are also supported; this allows resource scripts to be used to store server cluster-wide configuration information that can be used and managed the same way as any other resource. Microsoft Message Queuing (MSMQ) support has been enhanced to include support for triggers. This allows highly available applications to be built based on all of the features provided by the reliable messaging infrastructure.
Network Enhancements	Server clusters take advantage of important network enhancements. Enhanced logic for failover is now supported when there has been a complete loss of internal (heartbeat) communication; and the network state for public communication of all nodes is now taken into account before the quorum ownership decision is made. Media sense detection provides better failover protection. Because media sense is disabled by default, the network role is preserved and all IP address-dependent resources remain online.
Improved Storage Capabilities	Server clusters take advantage of powerful storage capabilities. Volume mount points are now supported on shared disks and work on failover, providing a flexible file system namespace. Client-side caching (CSC), also known as Offline Files, is now supported for clustered file shares and lets a client computer cache data stored on a clustered share. Distributed File Service (DFS) allows multiple file shares on different computers to be aggregated into a common namespace. DFS enhancements in Windows .NET Server 2003 include multiple DFS roots per DFS server, ability to use AD site costing to select the closest available server for a given path, improved scalability for DFS Root servers, dynamic determination of file server site locations and an enhanced UI. Shared disks can now be located on the same storage interconnect as the boot, pagefile and dump file disks. This allows a clustered server to have a single—or a single redundant—storage interconnect. NOTE: This is only available where vendors have configured and qualified such configurations.
Streamlined Operation	Server clusters take advantage of important operational capabilities. Databases and configuration data can be backed up and restored, while node failover supports failover for clusters with two or more nodes. Group affinity support provides improved performance and availability because applications are failed over to spare nodes before active nodes. Rolling upgrades from Windows 2000 to the Windows .NET Server 2003 Family ensure minimum downtime because only one node in a cluster has to be taken offline for upgrading. The cluster service account password can be changed dynamically without having to take cluster nodes offline. Resource deletions are done using Cluster Administrator or with Cluster.exe, without having to take the resource offline. A tool is provided that allows the password for the cluster service account to be updated

	while the cluster service remains on-line and running. An IT administrator can use this feature to change passwords on a node without rebooting the server. This results in improved high availability and uptime.
Easier Troubleshooting and Failure Recovery	A number of improvements have been made to server cluster log files to allow easier debugging and troubleshooting. These improvements include: cluster logs; setup logs; error levels; local server time stamp; GUID (globally-unique identifier) to resource name mapping and event log. When a chkdsk is run against a cluster disk, the chkdsk log is kept around, and the status from chkdsk is written to the cluster log. A new diagnostics tool is available in the Resource Kit (ClusDiag) that allows cluster logs and event logs from all nodes in the cluster to be correlated and compared. In the event of a disk failure, the Resource Kit contains a new tool (ClusterRecovery) that allows the disk resource to be reconstructed and the cluster state to be rebuilt.
Majority Node Set	Windows .NET Server 2003 provides the traditional cluster quorum mechanism, as well as a new quorum resource called "Majority Node Set." This quorum resource allows server clusters to be built without using a shared disk as the quorum device. Using this new quorum mechanism additional cluster topologies can be built; for example, server clusters with no shared disks. Majority Node Set also makes it easier to build and configure multi-site, geographically dispersed clusters.
Availability Metrics	Windows .NET Server 2003 provides a means to measure availability of an individual group in a cluster. Log cluster availability events are added to the Event Log with adequate timing information to be able to calculate the availability of a cluster Resource Group. This feature enables an administrator to assess availability of an individual group in a cluster. The cluster service will log group moves and online or offline events for success and failure in the system event log. In addition, inter-node clock skew events are written to the system event log. By analyzing the event log streams from all of the cluster nodes looking at the times between offline and online events (taking into account cross-node clock skews), the amount of time a group is online versus offline can be calculated.
Kerberos Support for Virtual Servers	Kerberos authentication can be enabled when clients access the resources of a cluster by means of a cluster virtual name. When this feature is enabled, a virtual computer object is created in Active Directory. This provides cluster-aware and Active Directory-aware applications with an object in Active Directory to publish service provider information specific to the virtual server on which they are hosted.
Multi-cast Heartbeats Between Nodes	Multi-cast heartbeats between nodes in a server cluster can reduce the amount of cluster heartbeat traffic between nodes in a larger cluster. This will help reduce network and computer Central Processor Unit (CPU) utilization. This feature is turned on by default. To modify the default configuration, use the command line utility and cluster.exe.
WMI Support for Server clusters	Server clusters provides Windows Management Instrumentation (WMI) support for cluster control and management functions, application and cluster state information. In addition, cluster state change events are propagated through WMI. Applications can also subscribe to WMI events that show information such as application failure and restart and node failure. This makes it easier for an administrator to manage and monitor the cluster.

Remote Scripting Host Support	The Cluster Resource Scripting Host simplifies the process of developing clustering applications. By providing a run-time environment that takes care of all complex issues, it allows for easy creation of new resource types. Windows Scripting Host support for cluster resources includes: • Resource health monitoring and instrumentation for applications and services • Simpler process of implementing a new resource type • Scriptable application instrumentation that simplifies the process of making the application cluster-aware • Run-time hosting environment • Reuse of existing Common Object Model (COM) automation servers
Storage Area Network (SAN) Boot	In the new Storage Area Network (SAN) technology, all of the disks in a cluster may be in the same storage fabric accessed through a single Host Bus Adapter (HBA). This feature allows all disks (except the boot disk, the system disk and disks containing page files) to be considered as shared disks regardless of the storage bus technology. This capability can be built into larger solutions by OEMs, IHVs and other software vendors.
Storage Area Network (SAN) Device Arbitration	The new Storage Area Network (SAN) technology is viewed as a method to provide data consolidation and ease of management. Bus reset, a disruptive action for nodes that share a SAN, is not a defined operation. This feature modifies the cluster arbitration mechanism in order to avoid bus resets where possible. The mechanism will try various options before the last alternative of a bus reset. After lower level drivers, such as SCSIPIRT and RAIDPORT, have implemented device arbitration, this feature will be able to decide reset options based on topology and storage type.
Encrypted File System on Clustered Disks	Windows .NET Server 2003 supports Encrypted File System (EFS) on clustered (shared) disks. The Encrypting File System is the technology used to store encrypted files on NTFS volumes. Encrypted files and folders are easy to use as they appear just like any other file or folder—transparent to authorized users but inaccessible to anyone else.

Network Load Balancing Features

Feature	Description
Network Load Balancing Manager	This new utility in the Windows .NET Server 2003 Family provides a single point of configuration and management for NLB clusters. NLB Manager can be used to: • Create new NLB clusters and automatically propagate cluster parameters and port rules to all hosts in the cluster. It can also propagate host parameters to specific hosts in a cluster. • Add and remove hosts, to and from NLB clusters. • Automatically add Virtual IP (VIP) addresses to TCP/IP. • Manage existing clusters by connecting to them or by loading their host information to a file and saving this information for later use. • Configure NLB to load balance multiple Web sites or applications on the same NLB cluster. This includes adding all cluster IP addresses to TCP/IP, and controlling traffic sent to specific applications on specific hosts in the cluster. • Diagnose improperly configured clusters. The NLB Manager can be started from the command prompt by typing nlbmgr.exe.

Virtual Clusters	This new feature in the Windows .NET Server 2003 Family can be used to: • Configure different port rules for different cluster IP addresses, where each cluster IP address corresponds to a Web site or application being hosted on the NLB cluster. • Filter out traffic sent to a specific Web site or application on a specific host in the cluster. • Pick and choose which host in a cluster should be used to service traffic sent to a specific Web site or application being hosted on the cluster.
Multi-NIC (Network Interface Card) Support	The Windows .NET Server 2003 Family binds NLB to multiple network cards and enables users to: • Host multiple NLB clusters on the same hosts while leaving them on entirely independent networks. • Use NLB for firewall and proxy load balancing in scenarios where load balancing is required on multiple fronts of a proxy or firewall.
Bi-Directional Affinity	The most common usage of bi-directional affinity is to cluster Internet Security and Acceleration servers (ISA) for proxy and firewall load balancing. NLB is commonly used together with ISA for server publishing. Bi-directional affinity creates multiple instances of NLB on the same host, which work in tandem to ensure that responses from published servers are routed through the appropriate ISA servers in a cluster. In order for this capability to be used, NLB needs to operate in a special mode that ties the NLB instances running on the inside and outside network interfaces of the ISA server and allows the NLB on the internal interface of an ISA Server to hash on a connections Destination Internet Protocol (IP) Address instead of the usual Source IP Address.
Internet Group Management Protocol (IGMP) Support	This new feature limits switch-flooding. Switch-flooding is caused by the NLB algorithm which requires that every host in an NLB cluster be able to see every incoming packet addressed to the cluster. IGMP-support conserves network resources by limiting flooding to only those ports on a switch that have NLB computers connected to them. Note: IGMP-support can only be enabled when NLB is configured in multicast mode.
IP Security Integration	IP Security integration allows a group of Network Load Balancing (NLB) servers to provide highly available Internet Protocol Security (IPSec)-based Virtual Private Network (VPN) services. This is also supported by down-level Layer Two Tunneling Protocol (L2TP) or IPSec clients. The Internet Key Exchange (IKE) protocol automatically detects the NLB service, so no additional administrator action is required to use this feature.

Summary

Clustering services in Windows .NET Server 2003 will provide dramatic improvements by enhancing existing features and offering important new options.

Installation and setup is easier and more robust. With pre-configurations, remote administration, and established defaults, a basic server cluster can be up and running more quickly, and with fewer reboots.

Integration of clustering services with Active Directory provides many benefits, including: a "virtual" computer object, Kerberos authentication and security, and tighter integration with other services that publish information to Active Directory.

Enhanced network features provide greater failover capabilities and high system uptime. Support and troubleshooting additions allow administrators to pinpoint failures, and possible future issues, using real-time monitoring tools.

More Information

Microsoft will publish a longer detailed technical overview of this Windows .NET Server 2003 technology on the Web when Release Candidate 1 of Windows .NET Server 2003 becomes available.

Link to these longer technical articles at

<http://www.microsoft.com/windows/netserver/techinfo/overview> .

File and Print Services

Introduction

At the heart of any IT organization is the ability to efficiently utilize file and print resources and keep them available and secure for users. As the network expands with greater numbers of users located either onsite, in remote locations, or even in partner companies, IT administrators face an increasingly heavier burden.

Building on the foundation established in Windows 2000 Server, the Windows .NET Server 2003 Family will deliver improved file and print functionality, allowing you to reduce overall total cost of ownership (TCO). The result: increased dependability, greater productivity, and enhanced connectivity.

Benefits

The Windows .NET Server 2003 Family will provide the following file and print benefits:

Benefit	Description
Increased Dependability	Windows .NET Server 2003 ensures higher reliability with new features such as Automated System Recovery (ASR), making it easier to recover your system, back up your files, and maintain maximum availability.
Greater Productivity	Windows .NET Server 2003 delivers an enhanced file system infrastructure, making it easier to utilize, secure, and store files and other essential resources. Employees benefit by always being able to access the resources they need or quickly recover files without costly assistance from an IT helpdesk.
Enhanced Connectivity	Windows .NET Server 2003 will provide new and enhanced features such as remote document sharing, improving connectivity within and across organizations.

New Features and Improvements

The Windows .NET Server 2003 Family will provide many enhancements to the file and print infrastructure:

- Enhanced file system features.
- Improved printing features.

Enhanced File System Features

Feature	Description
Remote Document Sharing (WebDAV)	A new feature in Windows .NET Server 2003, remote document sharing, increases 'connectedness' to your business through the WebDAV redirector. With the WebDAV redirector, clients can access files on Web repositories through file system calls. The Web Digital Authoring & Versioning (WebDAV) redirector is a new mini-redirector that supports the WebDAV protocol for remote document sharing over Hyper Text Transfer Protocol (HTTP). The WebDAV redirector supports the use of existing applications and allows file sharing across the Internet (through firewalls, routers, etc.) to HTTP servers.

Automated System Recovery (ASR)	A new feature in Windows .NET Server 2003, Automated System Recovery (ASR) improves productivity by enabling a one-step restore of operating system, system state, and hardware configuration in disaster recovery situations. Automated System Recovery (ASR) feature provides the ability to save and restore applications. This feature also provides the Plug and Play mechanism required by ASR to back up Plug and Play portions of the registry and restore that information to the registry.
Command-line Interface	Windows .NET Server 2003 will provide new command-line utilities for many disk management tasks including ability to grow basic disks, perform various disk and RAID configurations, shadow copy management, and file system tuning.
GUID Partition Table (GPT)	Windows XP 64-Bit Edition and the 64-bit versions of Enterprise Edition and Datacenter Edition support a new disk partitioning style, the GUID Partition Table (GPT). Unlike master boot record (MBR) partitioned disks, data critical to platform operation is located in partitions instead of unpartitioned or hidden sectors. In addition, GPT partitioned disks have redundant primary and backup partition tables for improved partition data structure integrity.
Higher Performance Defragmentation Tool	The Windows Defragmenter tool can increase disk performance by optimizing files on a volume. Defrag in Windows .NET Server 2003 is faster and more efficient than it was in Windows 2000 Server, plus it supports online defrag of the Master File Table (MFT) and can defrag NTFS volumes with any cluster size. Disk Defragmenter tool enhancements include: • File System API Set – The NTFS defragmentation APIs now operate with better performance and few special-case constraints • Graphical User Interface (GUI) – Provides efficient Shadow Copy support and exploits new APIs • Command Line – Provides a simple command line to assist with scripting efforts. There are command-line commands for several tasks, including defragmenting one volume at a time and analysis of the driver by using the GUI. The command line and GUI operation are mutually exclusive. The disk defragmenter is located under the Start Menu at All Programs, Accessories, System Tools.
Content Indexing	Content indexing is a fast, easy, and secure way for users to search for information locally or on the network. Users can search in files in different formats and languages, either through the Search command, on the Start menu, or through HTML pages that they view in a browser.
Enhanced Distributed File Service (DFS)	The Distributed File Service (DFS) helps you create one logical file system out of multiple physical systems, making your environment easier for users to use and more efficient in terms of equipment utilization. With DFS you can create a single directory tree that includes multiple file servers and file shares in a group, division, or enterprise that allows users to easily find files or folders distributed across the network. Using the Active Directory service, DFS shares can also be published as Volume Objects in the Active Directory and administration can be delegated. In Windows .NET Server 2003, DFS now offers a closest site selection capability where DFS uses Active Directory site metrics to route a client to the closest available file server for a given path. Plus, a single Windows .NET Server 2003 system can host multiple DFS roots. This reduces the administrative and hardware costs associated with managing

	multiple namespaces and multiple replicated namespaces.
Distributed File Service (DFS) Administration Improvements	This feature exposes more functionality of the File Replication Service (FRS) through a new Distributed File Service (DFS) Microsoft Management Console (MMC) Snap-in. Actions supported by this console include: • Removal of replication filtering • Ability to display all types of FRS configurations • Ability to change non-SYSVOL types of FRS configurations • Definition of FRS replica set • Creation of topologies such as full mesh, star and hub • Ability to specify schedule on individual connections • Ability to extend other MMC Snap-ins • An IT administrator can use this feature to manage system volumes
Windows Management Instrumentation (WMI) for Configuring DFS	This feature allows the creation, configuration and deletion of Distributed File Service (DFS) shares through Windows Management Instrumentation (WMI). A developer can use this feature to enable applications and scripts to create, modify and monitor DFS links, add new DFS folders to a DFS link, remove DFS folders from a DFS link and manage DFS replicas.
DFS File Replication Services (FRS)	File Replication Services (FRS) works in conjunction with DFS by replicating data on file shares, automatically maintaining synchronization between copies across multiple servers. A new feature in Windows .NET Server 2003, the DFS MMC UI allows configuration of replication topologies. The FRS service itself also has new features—compression of replication traffic and the ability to damp unnecessary replication traffic.
Enhanced Encrypting File System (EFS)	The Encrypting File System is the technology used to store encrypted files on NTFS volumes. Encrypted files and folders are easy to use as they appear just like any other file or folder—transparent to authorized users but inaccessible to anyone else. EFS is particularly beneficial for mobile users who may face a higher risk of computer loss or theft. An unauthorized person who tries to access encrypted files or folders is prevented from doing so, even if the intruder has physical access to the computer. EFS improvements in Windows .NET Server 2003 include the ability to authorize additional users to access encrypted files, the ability to encrypt offline files as well as store encrypted files in Web folders.
New Support for Antivirus Products	Windows .NET Server 2003, includes a special new kernel APIs intended to enable higher performance and reliability of third-party antivirus products. In addition, there is now a WHQL test suite and driver certification process for antivirus file system filter drivers.
Increased CHKDSK Performance	Because the NTFS file system has always been a true journaled file system, CHKDSK operations are rarely required. Fewer than 1 percent of unplanned outages require such checking. If, in the unlikely event a disk does need to be checked, CHKDSK performs substantially faster (1271% according to http://www.etestinglabs.com) than previous versions of Windows.
Remote Storage	Remote Storage uses criteria you specify to automatically copy little-used files to removable media. If hard-disk space drops below specified levels, Remote Storage

	removes the (cached) file content from the disk. If the file is needed later, the content is automatically recalled from storage.
Removable Storage	Removable Storage makes it easy to track your removable storage media (tapes and optical discs) and to manage the hardware libraries, such as changers and jukeboxes that contain them. Because removable optical discs and tapes are less expensive per megabyte (MB) than hard disks, Removable Storage and Remote Storage can decrease your costs.

Improved Printing Features

Feature	Description
Command-line Interface	Windows .NET Server 2003 provides a new command-line utilities for many tasks including printer management and configuration, job and queue control, port management, and driver management. Using a Windows Management Instrumentation (WMI) provider, scripts or batch files can be developed to manage printers in an unattended or automated manner.
Print Cluster Support	A new feature in Windows .NET Server 2003, Print Cluster support improves productivity by making it easier to install print drivers on server clusters. When installing a printer driver on a virtual cluster, Windows .NET Server 2003 automatically propagates the driver to all nodes of the cluster.
64-Bit Printing	Support for 64-bit drivers and applications is a new feature in Windows .NET Server 2003. "Point-n-print" provides client-server printing support for interoperability of 32-bit to 64-bit clients and servers. This feature provides the ability for 32-bit applications to be able to print using a 64-bit print server. An IT administrator running a 32-bit management application on a computer with 32-bit operating system can add, delete and configure ports of a 64-bit print server.
Wide Range of Devices	Windows .NET Server 2003 improves connectivity with built-in support for more than 3,800 new printer drivers.
Reliability Improvements	Windows .NET Server 2003 increases reliability of print servers by providing kernel mode driver blocking, giving administrators fine grain control of driver installation on the server.
Active Directory Enhancements	By publishing printers in Active Directory, Windows .NET Server 2003 enable users to quickly locate and connect to printers based on criteria such as location, ability to print color, or the speed of the printer.
Performance Improvements	Windows .NET Server 2003 improves performance over Windows 2000 by optimizing file spooling (read/write from disk) for higher print volume management. Users benefit by getting their documents faster.
Plug and Play Enhancements	Windows .NET Server 2003 improves your productivity by recognizing and adapting to hardware configuration changes automatically.
Easier Printer	You can easily monitor operation of local and remote printers. With System Monitor you

Management	can control counters for a variety of criteria, such as Bytes printed/second, job errors, or total pages printed.
Increased Performance for Network Printing	Standard Port Monitor, Microsoft's primary method for fast and robust printing to network attached printers, has been updated to provide better performance and richer device status. Windows .NET Server 2003 also now includes wireless (802.1X, Bluetooth) printing support. In addition, print drivers are downloaded automatically when client computers connect to print servers, simplifying printing across a network and saving time.
Broader Interoperability	Using AppleTalk, LPR/LPD, and IPX protocols, Windows Print Servers can accept jobs from other client operating systems such as Macintosh, UNIX, Linux, or Novell systems. Conversely, Windows-based client computers can print to servers running other operating systems.
Windows Management Instrumentation (WMI) Provider	The purpose of this feature is to add more functionality onto the existing Windows Management Instrumentation (WMI) provider for printing components. This includes an in-box scriptable interface for management of the major functions in printing, including: • Adding ports, drivers and printers to print servers • Updating printer drivers. • Using an active print trouble shooter to do operations such as take printers offline, put printers online, and purge print queues • Be notified of events such as spooler server stopped, and print configuration changes • Use a third-party management tool to manage print system components along with other operating system components • Share a printer as a network resource

Summary

The Windows .NET Server 2003 Family builds on the foundation of Windows 2000 with new feature and improvements that drive down the total cost of ownership. These File and Print services together with improved storage management functionality strengthen the dependability of your core infrastructure. Employees can be more productive due to less downtime and easy retrieval of files and resources. Finally, Windows .NET Server 2003 will allow everyone in your organization to stay better connected and take full advantage of the emerging platform for XML Web Services.

More Information

Microsoft will publish a longer detailed technical overview of this Windows .NET Server 2003 technology on the Web when Release Candidate 1 of Windows .NET Server 2003 becomes available.

Link to these longer technical articles at

<http://www.microsoft.com/windows.netserver/techinfo/overview> .

Internet Information Services 6.0

Introduction

Administrators and Web application developers demand a fast, reliable Web platform that is both scalable and secure. Internet Information Services (IIS) 6.0 and Microsoft Windows .NET Server 2003 introduce many new features for Web application server management; performance and scalability; availability, reliability, and security. Significant architectural improvements have been made to meet customer requirements.

This section provides an overview of the next generation of Web infrastructure capabilities available in the Windows Server family. It also describes the benefits and new technical features that are available when you deploy IIS 6.0.

Benefits from Deploying IIS 6.0

IIS 6.0 offers a wide variety of new features and technologies that make it more reliable, scalable, secure, manageable, and enabled for enhanced development.

Reliable and Scalable	IIS 6.0 is based on a new request processing architecture that provides an application isolation environment which enables individual Web applications to function within their own, self-contained Web service process. This environment prevents an application or site from stopping another and reduces the amount of time administrators need to spend restarting services to keep applications healthy. This capability enhances the availability of IIS by making the server harder to bring down. Scalability improvements and support include Network Attached Storage (NAS) support.
Secure	IIS 6.0 is fully locked down by default and includes an easy to use user interface for application enablement. Another security enhancement involves the new request processing architecture in IIS 6.0 which includes process recycling. In addition, IIS runs as a low privileged account by default, thereby containing worker processes.
Manageable	IIS 6.0 includes a variety of management tools to meet varying customer needs. IIS 6.0 offers pervasive administrative access, powerful administration capabilities and flexible configuration management options in an improved, easier to use interface. Administrators can make configuration changes and debug applications while services are running. IIS 6.0 also includes a variety of new and improved command-line tools.
Enhanced Development	Windows .NET Server 2003 offers an improved developer experience with ASP.NET and IIS integration. Building upon IIS 6.0, platform enhancements offer developers very high levels of functionality - rapid application development and a wide variety of languages to choose from. With Windows .NET Server 2003, the experience of ASP.NET and the .NET Framework is improved as a result of the improved process model integration. IIS 6.0 offers support for the latest Web standards, including XML, SOAP and IPv6.
Application Compatibility	IIS 6.0 has proven compatibility with most existing applications based upon engaging thousands of customers and ISVs. In addition, IIS 6.0 can optionally be configured to run in <i>IIS 5.0 isolation mode</i> which ensures maximum compatibility. Where issues have been identified for some solutions, workarounds are often made available on the Web.

New Features and Improvements

Internet Information Services (IIS) 6.0 in Windows .NET Server 2003 provides a number of new features and important improvements, including:

- New Request Processing Architecture
- New Security Features
- New Manageability Features
- New Performance and Scalability Features
- New Programmatic Features
- Platform Improvements

New Process Model

Feature	Description
New Request Processing Architecture	IIS 5.0 was designed to have one process, Inetinfo.exe, be the main Web server process which could farm requests out to one or more out-of-process applications (dllhost.exe). In comparison, IIS 6.0 has been redesigned into two new components that use a new kernel-mode driver. This allows IIS to separate core Web server code from application handling code. These three new components are a kernel-mode HTTP listener, called HTTP.sys; a user-mode configuration and process manager, called the Web Administration Service; and the application handler, which is loaded into a separate worker process. These worker processes in turn service requests for application pools in HTTP.sys. Preliminary testing has shown over 100% throughput gain over previous releases of Active Server Pages (ASP) for an ASP.NET benchmark on an eight processor server.
HTTP.sys and Kernel-mode Queuing	In IIS 6.0, HTTP.sys listens for requests and queues those requests up on the appropriate queue for each request. Each request queue corresponds to one application pool. Because no third-party code runs in HTTP.sys, it cannot be affected by crashes in user mode code that normally affect the status of the Web service. If something causes the user mode request processing infrastructure to terminate, HTTP.sys continues to accept and queue requests provided the Web service is still up and running. HTTP.sys continues to accept requests and queue them on the appropriate queue until there are no queues available, there is no space left on the queues, or the Web service has been shutdown. Once the Web service notices the crashed worker process, it starts a new one if there are outstanding requests still waiting to be serviced for the worker process's application pool. Thus, while there may be a temporary disruption in user mode request processing ability, an end user does not experience the failure because requests continue to be accepted and queued.
Web Administration Service (WAS)	Another key portion of the new IIS 6.0 architecture is the Web Administration Service (WAS). WAS is responsible for two main areas: configuration and process management. WAS makes up a core portion of the Web service where, like HTTP.sys, critical IIS 6.0 services reside and third-party code is never loaded. IIS 6.0 completely isolates third-party application code from the core Web server by keeping the critical Web server functionality such as configuration management and request queuing, in WAS and HTTP.sys and allowing application code to run in dedicated mini-Web server processes called worker processes.

Worker Process Isolation Mode	IIS 6.0 introduces worker process isolation mode, which runs all application code in an isolated environment, but without the performance penalty of the previous IIS versions. HTTP requests are routed to the correct application pool queue: User mode worker-processes serving a pool pull the requests directly from the kernel and eliminate the unnecessary process hops encountered when having to send a request to an out-of-process DLLhost and back again. In IIS 6.0, there is no longer any notion of in-process applications; all necessary HTTP application runtime services such as ISAPI extension support are equally available in any application pool. This design prevents a malfunctioning Web application or Web site from disrupting other Web applications (or other Web sites) served from other worker processes on that server. It is now possible to unload in-process components without having to take down the entire web service. The host worker process can be taken down temporarily without affecting other worker processes serving content. There is also benefit from being able to leverage other OS services available at the process level (for example CPU throttling), per application pool. Additionally, Windows has been re-architected to support many more concurrent processes than ever before.
Clean separation between user code and the server	All user code is handled by worker processes, which are completely isolated from the core Web server. This improves upon IIS 5.0 in that ISAPI's can and often are hosted in-process to the core Web server. If an ISAPI loaded in a worker process crashes or causes an access violation, the only thing taken down is the worker process that hosts the ISAPI. Meanwhile, WAS creates a new worker process to replace the failed worker process. The other worker processes are unaffected.
Multiple Application Pools	With IIS 5.0, applications can be pooled together out-of-process but only in one application pool – DLLHOST.EXE. IIS 6.0 worker process isolation mode allows customers to create multiple application pools, where each application pool can have a different configuration (like recycling configuration, etc.).
Better Support for Load Balancers	With the advent of application pools, IIS has a well defined physical separation of applications. This makes it quite feasible to run hundreds or thousands of sites/applications side-by-side on one Windows server. In this configuration, it is important that one problematic application does not affect other healthy applications. It is also desirable to be able to automatically communicate with load balancers/switches to route away only the traffic for a problematic application, while still allowing the server to accept requests for the other healthy applications. IIS 6.0 has a built in extensibility model that can fire events and commands when the Web Application Server infrastructure detects a specific application's failure. This configuration ability allows load balancers and switches to be configured to automatically stop routing traffic to problematic applications while still routing traffic to healthy applications.

Web Gardens	IIS 6.0 worker process isolation mode also allows multiple worker processes to be configured to service requests for a given application pool. By default, each application pool has only one worker process. However, an application pool can be configured to have a set of N equivalent worker processes share the work. This configuration is known as a Web garden because it is similar in nature to a Web farm, except that a Web garden exists within a single server. Requests are distributed by HTTP.sys among the set of worker processes in the group, based on matching the queue of incoming requests for an application pool against a queue of "requests for requests" from each of the set of processes in the Web garden. A benefit to Web gardens is that if one worker process gets bogged down, there are other worker processes available to accept and process requests.
Health Monitoring	WAS is capable of monitoring the health of worker processes by pinging the worker processes periodically to determine if they are completely blocked. If a worker process is blocked, WAS terminates the worker process and creates another worker process for replacement. Furthermore, WAS maintains a communication channel to each worker process and can easily tell when a worker process fails by detecting a drop in the communication channel.
Processor Affinity	Worker processes can have affinity to specific CPU's to take advantage of more frequent CPU cache (L1 or L2) hits.
Allocating Sites and Applications to Application Pools	In IIS 6.0, as in IIS 5.0, applications are defined as those namespaces that are labeled in the metabase with the AppIsolated property. Sites, by default, are considered to be a simple application—one where the root namespace "/" is configured as an application. An application pool can be configured to serve anything from one Web application to multiple applications up to multiple sites. Assigning an application to an application pool is as easy as configuring which application pool that application should be routed to in the metabase.
Demand Start	Application pools support on-demand starting when the first request for a URL in that part of the namespace arrives at the server. The IIS 6.0 application manager (contained within WAS) is the component that does on-demand process starting, and generally controls and monitors the lifecycle of worker processes.
Idle Timeout	An application pool can be configured to have its worker processes request a shutdown if they are idle for a configurable amount of time. This is done to free up unused resources. Additional worker processes are started when demand exists for that application pool (see the above section on Demand Start for more information).
Rapid-Fail Protection	When a worker process fails, it drops the communication channel with WAS. WAS detects this failure and takes action, which typically includes logging the event and restarting the process. In addition, IIS 6.0 can be configured so that if a particular application pool suffers multiple failures in a row, it can be automatically disabled. This is known as rapid-fail protection. Rapid-fail protection places the application pool in "out-of-service" mode and HTTP.sys immediately returns a 503 Service Unavailable out-of-service message to any requests to that portion of the namespace, including requests already queued for that application pool. An administrator can also explicitly put a namespace group into "out-of-service" mode, for example, if the application is being taken offline because of a serious application problem. This is done by stopping the application pool, which can be done either via IIS Manager or via script.

Orphaning Worker Processes	IIS 6.0 worker process isolation mode can be configured to “orphan” any worker process that it deems to be “terminally ill.” If a worker process fails to respond to a ping in a certain amount of time, WAS marks that worker process as terminally ill. Normally WAS terminates that worker process and starts a replacement. If “orphaning” is turned on, WAS leaves the “terminally ill” worker process running and starts a new process up in its place. WAS can be configured to run a command on the worker process (like attaching a debugger) when it “orphans” a worker process.
Recycling Worker Processes	IIS 6.0 worker process isolation mode can be configured to restart worker processes in an application pool periodically to manage faulty applications. Worker processes can be scheduled to restart based on: • Elapsed time • Number of requests served • Scheduled times during within a 24 hour period • A liveness ping, which the process must respond to (see “Health Monitoring” above) • Virtual memory usage • Physical memory usage • On demand
IIS 5 Isolation Mode	IIS 6.0 introduces worker process isolation mode in an effort to bring greater reliability, isolation, availability, and performance to Web servers. While worker process isolation mode offers increased isolation, reliability, availability, and performance, some applications may not work in its environment due to compatibility issues such as multiple-instance, session state persisted in process, or applications written as read raw data filters. Therefore, IIS 6.0 has the ability to switch to another process model, called IIS 5 isolation mode, to ensure compatibility.

New Security Features

Experience has taught us that it is impossible to pre-conceive every possible attack and proactively address all possible vulnerabilities. Yet, patterns have emerged in areas that hackers commonly exploit. As a result, several preventative measures are built into IIS 6.0 to make IIS out of the box more secure. In addition, work is being undertaken to make it easier to further “lock down” the site and more easily discover and apply security patches.

Feature	Description
Server Lockdown	In an effort to reduce the attack surface of your Web server, IIS 6.0 serves only static content after a default installation. Using the Web Service Extensions node in IIS Manager, Web site administrators can enable or disable IIS functionality based on the individual needs of their company. Administrators should be aware that IIS ships in a locked down state, where only static content (.htm, .jpg, .bmp, etc.) is served. Additional functionality such as Active Server Pages or Front Page Server Extensions will have to be enabled before their functionality works as expected.

Configurable Worker Process Identity	More and more customers run multiple applications or sites on one Web server. This puts certain requirements onto a Web server. If an Internet Service Provider hosts two companies or even competitors on one server he has to guarantee that these two applications run completely isolated from each other. More importantly: He has to make sure a malicious administrator for one application can't access data of the other application. Complete isolation is a must. IIS 6.0 can provide this level of isolation through the configurable worker process identity. Together with other isolation features like bandwidth and CPU throttling or memory-based recycling, IIS 6.0 provides an environment to host even the fiercest competitors on one Web server.
IIS Runs as a Low Privileged Account by Default	The worker process runs as NetworkService, which is a new built-in account with very few privileges. Running as a low privileged account is one of the most important security principles. The impact of potential security vulnerability can be extremely contained if the worker process has very few rights on the underlying system.
SSL Improvements	Performance – IIS 5.0 already provides the fastest software-based SSL implementation in the market. As a result, 50% of all SSL Web-sites run on IIS. IIS 6.0 will be even faster. We tuned and streamlined the underlying SSL implementation for even more performance and scalability. Remotable Certification Object – In IIS 5.0 it is not possible to manage SSL certificates remotely because the CAPI certificate store is not remotable. Because our customers manage 100's or even 1000's of IIS servers with SSL certificates, they need a way to manage certificates remotely. The CertObject allows customers to do this. Selectable Crypto-Service Provider Selectable Crypto-Service Provider – If SSL is enabled, performance may drop, because the CPU has to perform a lot of intensive cryptography. There are hardware-based accelerator cards that allow offloading of these cryptographic computations to hardware. They plug their own Crypto API provider into the system. IIS 6.0 makes it easy to select such a third-party provider.
Passport Integration	Windows.NET integrates Passport as a supported authentication mechanism for IIS 6.0. This integration provides .NET Passport authentication in the core Web server and uses .NET Passport version 2 interfaces provided by standard .NET Passport components. This allows customers to take advantage of the huge Passport customer base (150,000,000 +) without having to deal with account management issues like password expiration or provisioning.
URL Authorization	IIS 6.0 extends the use of a new Authorization framework that comes with Windows.NET servers by providing gatekeeper authorization to specific URLs. Additionally Web applications can use IIS 6.0 URL authorization in tandem with Authorization Manager to control access to the URLs comprising the Web application, and the application specific tasks and operations, from within the same policy store. Maintaining the policy in the same policy store allows administrators to manage access to the URLs and application features from a single point of administration while leveraging the store-level application groups and user-programmable business rules.

New Manageability Features

The typical Internet Web site no longer operates on just one server. Web sites now spread across multiple Web servers or across "Web farms," which are clusters of servers that are dedicated to delivering content, business logic, and services. Even intranet sites, especially those delivering Web

enabled line-of-business applications, have increased in number as businesses turn more and more to delivering applications over the Web. As remote administration becomes more common, there has been an increasing demand for improved API access and improved “to the metal” configuration support. With the Internet and intranet changes over the past few years, managing a Web site is no longer as simple as managing one or a few Web servers from an office but is an integrated and complex process.

IIS 6.0 introduces new features to improve the administration capabilities for administrators who manage IIS Web sites. IIS 6.0 includes a storage layer replacement of the metabase (configuration store), which allows for direct text editing of the metabase configuration in a robust and recoverable fashion. Furthermore, Windows Management Instrumentation (WMI) support and improved command-line support allow for Web site administration without the use of IIS Manager.

Feature	Description
XML Metabase	The metabase is a hierarchical store of configuration values used by IIS that incorporates rich functionality such as inheritance, data typing, change notification, and security. The metabase configuration for IIS 4.0 and IIS 5.0 was stored in a proprietary binary file, and was not easily readable or editable. IIS 6.0 replaces the proprietary binary file called MetaBase.bin, with plain text XML formatted files. The benefits of XML formatted plain text metabase files are as follows: Improved backup/restore capabilities on computers that experience critical failures • Improved troubleshooting and metabase corruption recovery • The metabase files can be edited directly using common text editing tools • Application configuration is exportable and importable at user-specified locations • Improved performance and scalability • The new XML metabase allows administrators to easily read and edit configuration directly without having to use scripts or code to administer the Web server. The new XML metabase also makes strides at improving performance and scalability. As far as these two areas are concerned, the new XML metabase has: • Comparable or better disk footprint size • Faster read times on Web server startup than the IIS 5.0 binary metabase • Equivalent write performance to the IIS 5.0 binary metabase
Automatic Versioning and History	The metabase history feature automatically keeps track of changes to the metabase that are written to disk. When the metabase is written to disk, IIS marks the new Metabase.xml file with a version number and saves a copy of the file in the history folder. Each history file is marked with a unique version number, which is then available for the metabase rollback or restore processes. The metabase history feature is enabled by default.
Edit While Running	IIS 6.0 allows the administrator to edit the MetaBase.xml file while IIS is running. New configuration can easily be added by opening MetaBase.xml in Notepad for example and typing in the new configuration for a new site or editing an existing site's configuration.

Import and Export Configuration	IIS 6.0 introduces two new Admin Base Object (ABO) methods, Import() and Export(), which allow the configuration from any node level to be exported and imported across servers. Secure data is protected via a user-supplied password similar to the new backup/restore support. These new methods are also available to ADSI and Windows Management Instrumentation (WMI) users, and through IIS Manager.
Server-Independent Backups	The new Admin Base Object (ABO) API is available for developers to backup and restore the metabase with a password. This allows administrators and developers to create server-independent backups. The session key is encrypted with an optional user-supplied password during backup and is not based on the machine key. When backing up the metabase, the system encrypts the session key with the password supplied by the user. When restoring, the supplied password decrypts the session key, and the session key is re-encrypted with the current machine key. This new restore method can also restore backups made with the old back up method and follows the same behavior the old restore method uses when a the session key cannot be decrypted. Windows Management Instrumentation (WMI) and ADSI support these methods. The existing metabase backup/restore UI also uses the new backup/restore method.
IIS WMI Provider	Windows 2000 introduced a new means of configuring the server and gaining access to important pieces of data such as performance counters and system configuration – Windows Management Instrumentation (WMI). To leverage WMI capabilities such as query support and associations between objects, IIS 6.0 now has a WMI provider which provides a rich set of programming interfaces that offer more powerful and flexible ways to administrate your Web server. The IIS WMI provider provides similar functionality to the IIS ADSI provider for editing the metabase.
Command-Line Administration	IIS 6.0 now ships supported scripts in the Windows\System32 directory that can be used to administer an IIS 6.0 Web server. These scripts, written in VB Script, use the IIS WMI Provider to get and set configuration within the metabase. These scripts are designed to do many of the most common tasks facing a web administrator from the command line without having to use a user interface.
New Web-based Administration Console	The IIS Remote Administration Tool (HTML) allows you to remotely administer IIS across the Internet or your intranet through the Web browser.

New Performance and Scalability Features

A new generation of applications puts a greater demand on performance and scalability attributes of Web servers. Increasing the speed at which HTTP requests can be processed and allowing more applications and sites to run on one server translates directly into fewer servers needed to host a site. It also means that existing hardware investments can be sustained longer while being able to handle greater capacity. Overall improvements include preliminary testing suggesting performance gains up to 100% higher throughput on an 8 processor server under particular workloads.

Feature	Description
HTTP.sys - New Kernel-Mode Driver	The new kernel mode driver, HTTP.sys, is a single point of contact for all incoming (server-side) HTTP requests. This provides high performance connectivity for HTTP server applications. The driver sits atop TCP/IP and receives all connection requests from the IP/port combinations it is configured to listen on. HTTP.sys is also responsible for overall connection management, bandwidth throttling, and Web server logging. Preliminary testing suggests performance gains of 200% better throughput on static content, and cached responses achieved up to 165% higher throughput compared to IIS5.0.
Caching Policy & Thread Management	IIS 6.0 has advanced heuristics built in to determine the cacheable hot-set of an application or set of sites. Just because an item is cacheable, sometimes it does not make sense to add that item to an in-memory cache as there is a cost to managing the item and the memory it consumes. Therefore, IIS 6.0 uses a new heuristic to determine which items should be cached on the basis of the distribution of requests that a particular application receives. This means that the Web server makes better use of the resources on the server while sustaining the performance on frequent requests meaning this its scalability improves. IIS 6.0 also has heuristics built-in to monitor the overall state of the server and makes decisions to increase/reduce concurrency on that basis. The central idea here is to be efficient in using concurrency. For example, when executing processor-bound requests, starting concurrent work is not always the best approach.
Web Gardens	A Web garden is an application pool that has multiple processes serving the requests routed to that pool. You can configure the worker processes in a Web garden to be bound to a given set of CPU's on a multi-processor system. Using Web gardens, Web applications have increased scalability because a software lock in one process does not block all the requests going to an application. If there are 4 processes in the Web garden, a specific software lock blocks roughly a quarter of the requests.
Persisted ASP Template Cache	Before ASP code gets executed in IIS 5.0, the ASP engine compiles an ASP file to an ASP template. These ASP templates are stored in process memory. If a site consists of numerous ASP pages, this cache de-allocates the oldest templates from memory to free space for new ones. With IIS 6.0 these templates are persisted on disk. If one of these ASP files gets requested again, the ASP engine loads the template instead of loading the ASP file and spending additional CPU compiling it again. Preliminary testing suggests performance improvements with IIS 6.0 and ASP due to persistent on-disk cache include greater than 50% higher throughput.
Large Memory Support for x86	For workload that requires a great deal of cached data, IIS 6.0 can be configured to cache up to 64 GB an x86 system.

Enhanced Development Experience and New Programmatic Features

IIS 6.0 provides several new features while continuing to build on the ISAPI programming model, including ISAPI support for custom errors, internal redirection (ExecuteURL), buffer and handle send, and improved Unicode support.

Feature	Description
ASP.NET and IIS Integration and Variety of Language Choices	Windows .NET Server 2003 offers an improved developer experience with ASP.NET and IIS integration. Building upon IIS 6.0, platform enhancements offer developers very high levels of functionality - rapid application development and a wide variety of languages to choose from. With Windows .NET Server 2003, the experience of ASP.NET and the .NET framework is improved as a result of the improved process model integration in IIS 6.0. IIS 6.0 offers support for the latest Web standards, including XML, SOAP and IPv6.
ExecuteURL	ExecuteURL provides functionality to replace almost all read raw data filters. The most common customer scenario for developing read raw data filters is that they want to examine or modify the request entity body before the target URL processes it. Currently the only way to see the entity body of a request (if you are not the target URL) is through read raw data notifications. Unfortunately, writing an ISAPI filter to accomplish this goal can be exceedingly difficult, or even impossible in some configurations. ISAPI extensions, on the other hand, provide functionality for easy retrieval and manipulation of the entity body. ExecuteURL allows an ISAPI extension to process the request entity body and pass it to a child request, meeting the needs of nearly all read raw data filter developers.
Global Interceptors	ExecuteURL allows IIS 6.0 to implement ISAPI request interceptors that can intercept, change, redirect, or deny every incoming HTTP request for a specific URL space. IIS 5.0 already supports one ISAPI extension intercepting all requests with a single wildcard (*) scriptmap, configured by editing the application mappings for an application. In IIS 6.0, the single wildcard (*) scriptmap concept is extended to allow a multiple execution of global interceptors.
VectorSend	Implemented as a server support function for ISAPI's, VectorSend allows developers to put together a list of buffers and file handles to send, in order, and then hand off to IIS 6.0 to compile the final response. HTTP.sys compiles all the buffers and/or file handles into one response buffer within the kernel and then sends it. This frees the ISAPI from having to do any of this buffer construction or multiple write-clients.
Caching of Dynamic Content	Another new feature is the implementation of a kernel mode cache for dynamic content. The benefit to this feature is that many customers have programmatically created content that doesn't change. In previous versions of IIS, the requests had to transition from kernel mode to user mode for every dynamic request and the responses had to be regenerated. Eliminating this transition and pulling the cached content from the kernel mode cache results in a marked performance improvement.

ReportUnhealthy	A new ISAPI extension ServerSupportFunction called HSE_REQ_REPORT_UNHEALTHY allows an ISAPI extension to call into the IIS 6.0 worker process to request that worker process be recycled. Developers can use this new server support function to request a recycle if their application ISAPI becomes unstable or enters an unknown state for any given reason. Note that in order to enable recycling after an ISAPI calls HSE_REQ_REPORT_UNHEALTHY, health monitoring should be turned on. When calling HSE_REQ_REPORT_UNHEALTHY, the developer can also pass in a string representing the reason why the ISAPI is calling HSE_REQ_REPORT_UNHEALTHY. This string is then added to the event the worker process publishes to the Application event log.
Custom Errors	ISAPI developers no longer need to generate their own error messages. Instead, they can plug into the custom error support built into IIS through a new ServerSupportFunction called HSE_REQ_SEND_CUSTOM_ERROR.
Unicode ISAPI	Unicode becomes more and more important in a global economy. Due to the non-Unicode structure of the HTTP protocol, IIS 5.0 limits the developer to the system code page. With UTF-8 encoded URLs, Unicode becomes possible. IIS 6.0 allows customers to get to Server Variables in Unicode and adds two new ServerSupportFunctions to allow developers to get to the Unicode representation of an URL. International customers with multi-language sites benefit from this feature and improved development experience.
COM+ Services in ASP	In IIS 6.0, the IIS and COM+ teams have separated the COM+ services from components and allow ASP applications to use a set of COM+ services. In addition to those services available in COM+ on Windows 2000, a few new services have been added and are supported in ASP: Fusion Support – Fusion allows an ASP application to use a specified version of a system runtime DLL or classic COM component. Partition support – COM+ partitions allow an administrator to define a different configuration of a single COM+ application for different users. This configuration includes security and versioning information. For more information about COM+ partitions, consult the COM+ documentation. Tracker support – When enabled, the COM+ tracker allows administrators to monitor what code is running within the ASP session and when. This information is extremely helpful to debug ASP applications. For more information about the COM+ tracker, consult the COM+ documentation Apartment model selection – ASP, through COM+, allows developers to determine which threading model to use when executing the pages in an application. By default, ASP uses the Single Threaded Apartment. However, if the application uses poolable objects, it can be run in the Multi-Threaded Apartment.

Platform Improvements

In addition to the features described above, IIS 6.0 has made a number of improvements to the platform overall. Among other things, these features make IIS a more compelling platform globally in addition to the features noted above.

Feature	Description
Win64 Support	The complete Windows .NET Server 2003 Family code base is compiled for 32-bit and 64-bit platforms. Customers who demand highly scalable applications can take advantage of an operating system that runs and is supported on these two platforms.
IPv6 Support	IPv6, or Internet protocol version 6, is the next generation IP protocol for the Internet. The Windows.NET Server Family now implements a production ready IPv6 stack. On servers where the IPv6 protocol stack is installed, IIS 6.0 will automatically support handling HTTP requests that arrive over IPv6.
Granular Compression	On a congested network it is useful to compress responses. In IIS 5.0 compression was an ISAPI filter and could only be enabled for the whole server. IIS 6.0 allows a much more granular configuration (file level).
Resource Accounting and Quality-of-Service (QoS)	Quality-of-Service (QoS) ensures that particular components of the Web server or individual content served by that server don't take over all server resources, like memory or CPU cycles. It allows the administrator to control the resources being used by particular sites, application pools, the Web service as a whole, etc. Basically, it ensures a certain <i>quality of service</i> that other services/sites/apps on the system receive by limiting the resources consumed by particular Web sites/apps (and/or the Web service as a whole itself).
Logging Improvements	UTF-8 Logging Support – With additional Unicode and UTF-8 support, IIS 6.0 now supports writing log files in UTF-8 instead of just ASCII (or local code page). Binary Logging – Binary logging allows multiple sites to write to a single log file in a binary, non-formatted manner. This new logging format will offer improved performance over current text-based (W3C, IIS, and NCSA) logging formats since the data doesn't have to be formatted in any specific manner. Logging of HTTP Substatus Codes – IIS 6.0 also supports the ability to log HTTP substatus codes in W3C and Binary logging formats. Substatus codes are often helpful in debugging or troubleshooting since IIS returns specific substatus codes for specific types of problems.

FTP Improvements	Traditionally, ISP/ASP customers have used FTP to upload their Web content because of its easily availability and wide adoption. IIS 6.0 allows the isolation of users into their own directory, thus preventing users from viewing or overwriting other users' Web content. The user's top-level directory appears as the root of the FTP service, thus restricting access by disallowing further navigation up the directory tree. Within the user's specific site, the user has the ability to create, modify, or delete files and folders. The FTP implementation is architected across an arbitrary number of front-end and back-end servers, which increases reliability and availability. FTP can be easily scaled based on the addition of virtual directories and servers without impacting the end users. PASV FTP requires the server to open a data port for the client to make a second connection. This is a separate connection than the typical port 21 that is used for the FTP control channel. The port range used for PASV connections is now configurable with IIS 6.0. This feature can reduce the attack surface of IIS 6.0 FTP servers by allowing administrators to have more granular control over the port ranges that are exposed over the Internet.
Improved Patch Management	Windows.NET server has greatly improved patch management. In fact, the following features have been added to improve the server, such as: No service interruption while installing patches – The new process model in IIS 6.0 includes process recycling, which means an administrator can easily install most IIS hotfixes and most new worker process DLLs without any interruption of service. Auto Update version 1.0 – Auto Update will provide three options to customers: Notify patch availability the moment it's available, Download patch and notify the availability of the patch, and Scheduled Install. Scheduled install allows the patch to be downloaded and automatically installed at a time decided by the administrator. Windows Update Corporate Edition – Many IT departments do not allow their users to go to the public Windows Update site as they do not want users to install security patches and other windows update packages without them being tested in a standard operating environment. Corporate Windows Update will now allow them to first run quality assurance tests on the patches that are required by the organization and once the patches have cleared the tests they would be placed on Corporate Windows Update server behind the firewall and all computers inside the firewall could then pick up the patch from this server. Resource Free DLLs – Windows has now separated the localization resources from the actual implementation and this has increased our turn around time to come up with fixes across 30 languages.

Summary

IIS 6.0 offers many new features to increase Web server reliability, manageability, scalability, performance, and security. With the XML metabase, administrators can transfer server configuration information between computers. The XML metabase also allows for remote administration. Worker process isolation mode protects the core of IIS from faulty applications and Web sites. In addition, IIS 5 isolation mode remains available for applications providing greater choice to administrators. IIS 6.0 introduces more command-line scripts, and the WMI provider uses COM object interfaces to provide access to IIS metabase data in a similar, yet in a more manageable manner than ADSI. With all these new improvements, IIS 6.0 can host thousands more Web sites per server than IIS 5.0 in addition to

better throughput and improved startup time. The improvements, features, and new architecture make IIS the most reliable, robust, and manageable Web server available.

More Information

Microsoft will publish a longer detailed technical overview of this Windows .NET Server 2003 technology on the Web when Release Candidate 1 of Windows .NET Server 2003 becomes available. Link to these longer technical articles at

<http://www.microsoft.com/windows.netserver/techinfo/overview> .

Management

Introduction

While computing has proliferated on desktops, laptops, and portable devices, the real cost of maintaining a distributed personal computer network has grown significantly. This total cost of ownership (TCO) includes not only the initial cost of hardware and software, but deployment expense, hardware and software update costs, training, day-to-day maintenance, and technical support as well.

The Windows .NET Server 2003 operating system builds on the foundation of Windows 2000, letting you increase the value of your existing investments while lowering overall computing costs. Easier to deploy, configure, and use, Windows .NET Server 2003 will provide centralized, customizable management services to reduce TCO. This section provides an overview of benefits, new features, and improvements for management services in Windows .NET Server 2003.

Benefits

Windows .NET Server 2003 will provide the following benefits.

Benefit	Description
Dependable	Windows .NET Server 2003 extends the reliability and availability of management tools introduced in Windows 2000 with improvements in key features such as Windows Management Instrumentation, Group Policy, and Resultant Set of Policy (RsoP). For example, new policy settings enable administrators to more easily manage environments in order to lock down desired configurations for groups of users throughout an organization.
Greater Productivity	With IntelliMirror® management services, users' applications, data, and settings are available to them regardless of where they log on, enabling them to get more done. And applications can be remotely installed and upgraded. Because organizations can deploy and manage customized desktop configurations, they spend less money supporting users on an individual basis. Users get the flexibility they need to do their jobs without having to spend time configuring their system on their own.
Connected	Improvements such as WMI command line management and remote management capabilities deliver unprecedented flexibility for administrators. Simplified folder redirection and more robust roaming capabilities enhance connectivity for users across an organization. And with cross forest support, organizations can achieve more interoperability scenarios, enabling increased flexibility.

New Features and Improvements

Windows .NET Server 2003 will provide the following:

- Improved Policy Setting Management Features
- Powerful Deployment Tools and Services
- Robust Command-line Management
- Windows Update
- Secure Software Update Services
- Integrated Solutions for Enterprise Class Management

Improved Policy Management Features

Windows .NET Server 2003 improves the way administrators can use Group Policy to control a wide range of configuration issues such as users' desktops, settings, security, roaming profiles, start menu options, and so forth.

Feature	Description
Group Policy Management Console	Expected to be freely available on the Microsoft Web site shortly after the release of Windows .NET Server 2003, the Group Policy Management Console (GPMC) will provide the new framework for managing Group Policy. With GPMC, Group Policy becomes much easier to use, a benefit that will enable more organizations to better utilize the Active Directory service and take advantage of its powerful cost saving features. For example, GPMC enables backup and restore of Group Policy objects (GPOs), import/export and copy/paste of GPOs, reporting of GPO settings and Resultant Set of Policy (RSoP) data, use of templates for managed configurations, and scriptability for all GPMC operations. For example, with import and copy paste of GPOs, administrators can maintain pre-built versions of GPOs for various configurations (highly managed desktops, laptops, Terminal Services on Windows .NET Server 2003, Exchange Servers, etc) and rapidly deploy them throughout their organization as needed. In addition, GPMC lets administrators manage Group Policy for multiple domains and sites within a given forest, all in a simplified user interface (UI) with drag-and-drop support. And with cross-forest trust, administrators can manage Group Policy across multiple forests from the same console. GPMC can manage Group Policy for Windows 2000 or Windows .NET domains.
Resultant Set of Policy (RSoP)	The Resultant Set of Policy feature in Windows .NET Server 2003 simplifies policy implementation and troubleshooting. RSoP allows administrators to determine the net effect of how policy settings are applied to users and computers. This tool allows an IT administrator to determine the resulting set of policy for a given user or computer in both an actual and a what-if scenario. The logging mode allows an IT administrator to examine what was actually processed on a given computer. The planning mode allows an IT administrator to perform "what if" analysis for a specified location in the directory, security group membership and WMI filtering properties. Resultant Set of Policy is available by the Active Directory Users and Computers MMC snap-in or by the Resultant Set of Policy MMC snap-in. It will also be integrated into the upcoming Group Policy Management Console
WMI Filtering	Windows Management Instrumentation (WMI) Filtering enables administrator to determine whether to apply a Group Policy Object (GPO) to a specific computer or user based on WMI properties of the target computer/user. This is similar in concept to the Security Group filtering that was implemented in Windows 2000.
New Policy Settings	Support for approximately 200 new policy settings have been to Windows.NET Server since Windows 2000. These policy settings provide the capability to customize and control the behavior of the Operating System for groups of users. These new policy settings affect functionality such as Control Panel, error reporting, Terminal Services, Remote Assistance, networking and dial-up connections, Domain Name System (DNS), network logon, Group Policy and roaming profiles.

Cross-Forest Support	The cross-forest feature in Windows .NET Server 2003 enables several new scenarios that Group Policy supports. While Group Policy Objects can only be linked to sites, domains, or OUs within a given forest, Windows.NET Group Policy successfully supports these new interoperability scenarios. For example, it is possible for a user in forest A to log on to a computer in forest B, each with their own sets of policy. Alternatively, settings within a GPO can reference servers in external forests, for example software distribution points..
Software Restriction Policies	The increased role of the Internet increases security threats to your network from viruses. With software restriction policies, organizations can protect their computer environment from suspect code by identifying and specifying the applications that are allowed to run. This feature provides a policy-driven mechanism to identify software running in a domain and control its ability to execute. It can identify software that is hostile or unwanted and prevent it from executing on computers running Windows XP and Windows .NET Server 2003 Family. This allows you to improve management of computers running Windows XP and Windows .NET Server 2003 Family in a way that allows better defenses against viruses, Trojans and unwanted applications. This feature also allows you to limit the software that runs on highly managed workstations (such as kiosks, task stations, or application stations) to only a certain list of software. This can help improve system stability and integrity for these computers. This feature is run from the Group Policy Object Editor.
Enhanced User Interface in the Group Policy Object Editor	Policy settings are more easily understood, managed, and verified with Web-view integration in the Group Policy Object Editor. Clicking on a policy instantly shows the text explaining its function and supported environments such as Windows XP only or Windows 2000.
Folder Redirection Enhancements	Administrators can now choose to redirect users' My Documents folder to the user's home directory.
Enhancements to Group Policy-based Software Distribution	Microsoft has implemented the following enhancements in .NET Server. Administrators can now choose to assign applications to users and have them either fully installed at logon, or on demand when the user starts the application. The option for this support is in the Software Settings node of the Group Policy Object Editor. Administrators can now specify a URL that will appear in the user's Add or Remove Programs applet that will point to support information.

Powerful Deployment Tools and Services

Windows .NET Server 2003 includes new technologies and features that ease the task of deployment.

Feature	Description
Remote Installation Services (RIS)	Administrators can use RIS servers using Risetup and RIPrep to deploy all versions of Windows 2000, Windows XP Professional, and all versions of Windows .NET Server 2003 (except Windows 2000 Datacenter and Windows .NET Server 2003, Datacenter Edition.) In addition, administrators can use RIS servers using Risetup to deploy the 64-bit version of Windows .NET Server, Enterprise Edition. Automated deployment is further enhanced with tighter security, improved performance to major components in RIS, such as Trivial File Transfer Protocol (TFTP), and HAL filtering to

	ensure that images are recognized only be computers with a compatible Hardware Application Layer (HAL). Administrators can save more time with the OS Choice Wizard, which can run in its entirety without administrator intervention. These and other improvements in RIS were designed to enable faster and more efficient automated deployment, resulting in lower TCO. RIS support for recovery console allows access to network files from the recovery consoles.
User State Migration	Migrating files and settings for multiple users in a corporate environment is made easier with the User State Migration Tool (USMT). "State" refers to the user's settings, files and documents. USMT aids deployments of Windows operating systems because it provides a means for an IT administrator to capture and restore this information when deploying new operating systems. This helps reduce time for the user after the new operating system is deployed because the users do not have to reconfigure desktop settings for such things as E-mail server, proxy server, and desktop color scheme desktop wallpaper. USMT is a command line tool that gives administrators flexibility to specify which settings should be restored. This command line tool is driven by INF files that can be customized. The default INF files migrate the majority of the shell settings, Internet and E-mail connectivity settings and common Office file types. Supported sources for the migration include Windows 95, Windows 98, Windows Millennium Edition, Windows NT 4.0, Windows 2000, Windows XP and Windows .NET Server 2003 Family. Windows XP and Windows .NET Server 2003 Family are the only supported destinations for the migration.
Windows Installer	Managing software applications in a corporate environment has traditionally burdened organizations with high costs. Now with Windows Installer, administrators can standardize and greatly simplify the process of customizing installations, updating and upgrading applications, and resolving configuration problems. Windows Installer can also manage shared resources, enforce consistent file version rules, and diagnose and repair applications at runtime. The result: significantly lower TCO for managing applications. Windows Installer includes several notable features running on Windows .NET Server 2003, including: • Digital Signature Support and Software Restriction Policy: This feature enables Windows Installer Packages to be digitally signed. This also allows Windows Installer Packages to honor the new Software Restriction policy settings for specifying what applications can be used. • Improved Reinstall and Patching Support: The Windows Installer version 2.0 has made a number of improvements to reinstalls and patching that increase the performance and reliability of this operation. The main improvements involve reducing the number of files that need to be copied by using file hashes and limiting the cases in which the installer needs to resolve the source for an application. • Support for 64-bit Applications: This feature enables 64-bit Windows Installer Packages to include both 32-bit and 64-bit components. The installer will correctly install and register 32-bit components with the WOW64 sub-system when they are installed. • Win32® and Common Language Runtime Support: This feature enables Windows Installer Packages to include assemblies. These assemblies can be installed globally to the computer in the Assembly store or privately to an application.

Robust Command-line Management

Windows .NET Server 2003 includes improved command-line management tools that allow administrators to complete most tasks without having to use a graphical user interface. This can increase efficiency for administrators desiring to use command-line functionality to automate common tasks.

Feature	Description
Ready to Use	Solutions are ready to use "out of the box" with little or no extra coding required. All tools have a consistent, standard syntax with easy access to command line documentation (/? Help text) as well as a comprehensive HTML Help file, "ntcmds.chm".
Remote Management	All new tools support remote server operation by means of the /S parameter (remote system name, for example, /S MyServer) as well as run under Telnet and Terminal Services, enabling fully remotable command-line management.
Scriptable	Administrators can use batch files or scripts at the command line to create customized management solutions and automate common tool usage.
WMI Command-Line Support	WMIC, a WMI command-line interface, is a powerful tool that gives administrators the precision to perform many WMI-related tasks such as retrieving information from a local computer, remote computer and from multiple computers in a single command. This utility includes a set of commands and control functions to facilitate management of a Windows environment. As such, the utility follows standard DOS and UNIX conventions. The WMIC interoperates with existing shells, utility command, and can be easily extended by scripts, or other administration-based applications. The WMI infrastructure is accessible by the command line utility throughout intermediate facilitators, called Aliases. Aliases are used to capture the features of a WMI class relevant to some specific task such as disk or network administration. Aliases can be used to rename classes, rename properties and methods, arrange properties in named formats that include property values and are formatted in a manner appropriate to some specific presentation strategy or function. This feature includes the ability to: • Define aliases, add output formats, and create and execute scripts. • Browse the WMI schema and query its classes and instances. • Get information from a local computer, remote computer and from multiple computers in a single command. • Given the current set of WMI providers, WMIC provides read access to approximately several thousand management variables, write access to approximately a few hundred management variables and to some management functions.

Windows Update

Millions of users each week use Windows Update as a way to keep their Windows systems up-to-date. Windows Update allows a user to connect to www.windowsupdate.com, where their computer will be evaluated to see which updates need to be applied to keep their system up-to-date, as well as any critical updates that will keep their system safe and secure. Windows Update also extends these services with Critical Update Notification, and Automatic Updates.

Feature	Description
Microsoft Windows Update Services Catalog Site	Administrators can download specific patches and drivers for distribution by using SMS or other management tools. See http://windowsupdate.microsoft.com/catalog .
Windows Update Consumer Site	Designed primarily for consumers or users in a lightly managed network environment, this Windows Update site delivers updates to individual computers accessing the Web site. This feature can be turned off or managed by using Group Policy. See http://windowsupdate.microsoft.com .
AutoUpdating	Administrators can automatically download and install critical updates such as security patches, high impact bug fixes and new drivers when no driver is installed for a device. AutoUpdate helps IT managers better manage the deployment and installation of critical Software Updates as well as consolidate multiple reboots into a single one. Compatible with corporate hosted Software Update servers, AutoUpdate will provide administrators with greater control of updates. Automatic updates can be configured automatically over the Internet or administered in-house. This feature also includes: • Detection: Automatic Updates (AU) uses the Windows Update control to scan the system and decide which updates are applicable to a particular computer. • Downloads: AU uses its innovative bandwidth-throttling technology for downloads. Bandwidth throttling uses only idle bandwidth so that downloads will not interfere with or will not slow down other network activity, such as Internet browsing. • Install: AU uses the Windows Update control for installing downloaded updates. • Security: The AU service checks user security privileges on each method call. It will only process calls coming from administrator user sessions. • Resolving user collisions: The service will allow the automatic update client to run only for one administrative user at a time.
Dynamic Update	Dynamic Update is designed to deliver emergency fixes to address any issues at setup time such as new drivers that are required but not available on the CD. This feature provides application and device compatibility updates, some driver updates, and emergency fixes for setup or security issues at operating system Setup time. After the need for a Dynamic Update package has been determined by Microsoft, it is provided from Windows Update. Internet access and minimally Internet Explorer 4.01 are required to download a Dynamic Update package.
Driver Services	Windows .NET Server 2003 enables administrators to get the latest certified drivers to users through Web sites and integration with device manager and Plug and Play services.

Secure Software Update Services

Microsoft Software Update Services is an online extension of the Windows operating system that keeps Windows-based systems (desktop and servers) up to date with security patches and critical updates.

Feature	Description
Microsoft Software Update Services	Because many corporations do not want their systems or users going to an external source for updates without first testing these updates, Microsoft will be providing an installable version of Windows Update for inside your corporate firewall. This Microsoft Software Update Services (SUS) will allow customers to install a service on an internal server—running Windows 2000 Server or Windows .NET Server 2003—that can download all "critical" updates as they are posted to Windows Update. Administrators will also receive email notification when new critical updates have been posted so they can prepare for them. This will allow administrators to very quickly and easily get the most critical updates to computers running Windows 2000 Server, Windows 2000 Professional, or Windows XP Professional. Client computers require the new Automatic Updates client, and can be configured centrally using Group Policy to automatically download and install approved updates. Note: Microsoft Software Update Services can only be used to distribute security patches and critical updates including security roll-ups. Microsoft Software Update Services is scheduled to be made available free of charge as a downloadable add-on in the second quarter of 2002.

Extending Windows .NET Server 2003 with other Management Products

The Windows .NET Server 2003 platform is at the core of Microsoft's vision for managing the enterprise. Its out-of-the-box management infrastructure and technologies enhance desktop management, streamline server administration, and simplify software deployment. Building on top of this infrastructure, Microsoft offers three solutions for enterprise-class management of Windows-based desktop and server systems.

Product	Description
Systems Management Server 2.0	Provides system inventory, enterprise-class software distribution and diagnostics.
Microsoft Operations Manager 2000	Delivers enterprise-class event and performance management for Windows-based environments of all sizes.
Application Center 2000	Helps deploy and manage high-availability Web applications built on the Microsoft Windows platform.

Additional Features

Feature	Description
Domain Rename	This feature supports changing the Domain Name System (DNS) and/or NetBIOS names of existing domains in a forest such that the resulting forest is still "well formed". The identity of a renamed domain represented by its domain Globally Unique ID (GUID) and its domain Security ID (SID) will not change. In addition, a computer's domain membership does not change as a result of the holding domain being renamed. This feature is particularly useful in scenarios where a corporation must change the

	names of domains. This feature might be used, for example, when a corporation undergoes a legal name change, or when companies merge and want to have a consistent nomenclature. Using Domain Rename is much more efficient than traditional methods, which may involve creating a new domain and migrating all the user and computer objects to the new domain. Although this feature provides a supported means to rename a domain, it is neither viewed nor meant to be a routine IT operation. Domain Rename will cause a service interruption requiring every Domain Controller to be rebooted. Domain rename will also require that every member computer of the renamed domain must be rebooted twice.
Headless Server	A headless server is one that can be completely administered remotely and therefore does not require local keyboard, mouse or video card and monitor. Windows provides many remote management tools for use when the server is functioning, such as Telnet, administration through Terminal Services, Windows Management Instrumentation (WMI), and Windows Scripting Host. Emergency Management Services (EMS) provides a mechanism to manage the server with no local keyboard mouse or monitor when Windows is not functional, such as when Windows is loading, a blue screen has occurred, during Setup, when the server is unavailable on a network, and during Remote Installation Services.
IntelliMirror	To help reduce costs, administrators need the highest levels of control over portable and desktop systems. IntelliMirror provides this control on client systems running Windows 2000 Professional or Windows XP Professional. You can use IntelliMirror to define policies based on business roles, group memberships, and locations. With these policies, Windows 2000 Professional desktops and Windows XP Professional desktops are automatically reconfigured to meet a specific user's requirements each time that user logs on to the network, regardless of where the user logs on.
Configure Your Server Wizard	The Configure Your Server Wizard makes it easier to set up a server by helping guide users in installing optional components that they choose during the Windows setup. This feature provides: • Ability to set up the first server on a network by automatically configuring Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), and Active Directory using basic default settings • Help for users to configure member servers on a network, pointing to the features they need to set up a file server, print server, Web and media server, application server, RAS and routing, or IP address management server • Adding Terminal Services as a server role • Adding the ability to install a Hypertext Markup Language (HTML) User Interface for the administration of Web servers and Network Attached Storage (NAS) servers. • A method to Configure Your Server and the Network Address Translation (NAT) of Routing and Remote Access Service (RRAS)
Microsoft Management Console	Microsoft Management Console (MMC) can be used to arrange administrative tools and processes within a single interface. You can also delegate tasks to specific users by creating preconfigured MMC consoles for them. The consoles provide the users with the tools that you select.
Password Backup and Restore	The new Password Backup/Restore Wizard provides a means to create a backup disk that can be used to reset a user's password. This feature provides the user a secure

	mechanism to reset their password without administrative intervention. The user's password is not stored on the backup disk and the disk can only be used to reset the password on that particular user account.
Remote Assistance	You can use Remote Assistance to remotely control a computer. If you have an invitation, Remote Assistance is a convenient way for you to connect to a remote computer from a computer running Windows XP or any product in the Windows .NET Server 2003 Family. After you are connected, you will be able to view the remote computer's screen and chat in real time. You can even use the mouse and keyboard to work on the remote computer, providing that the person requesting assistance allows you. This feature enhances peer-to-peer help experience by allowing users and support professionals to remotely view and control a computer for any support task. Chat and file transfers are also available during Remote Assistance sessions.
Remote Desktop for Administration	With Remote Desktop for Administration (formerly known as Terminal Services in Remote Administration mode), you can administer a computer from virtually any computer on your network. Based on Terminal Services technology, Remote Desktop for Administration is specifically designed for server management. Terminal Services now allows two different kinds of access to the server desktop for remote administration. As with Windows 2000, a user can create a remote session on the server, independent of the server console session. Up to two such sessions may be created concurrently, though it is advisable to ensure that only a single administrator use the computer at one time. In addition, the operating system now allows an administrator to connect remotely to the server console. When this is done, the console is locked at the physical device. To end the remote console session and bring console activity back to the physical server, simply enter the user credentials at the console.
Troubleshooting Diagnostic Tool	This feature provides a troubleshooting diagnostic tool that can help troubleshoot problems with the operating system by automating the standard troubleshooting steps. Users can complete basic troubleshooting steps from one location. The tool does this by using a series of check boxes to apply step-by-step system changes and it enables more advanced troubleshooting and problem resolution.
VT-UTF8 Support for Hyperterminal	This feature provides support for the terminal type VT-UTF8 (Unicode Transformation Format 8 in HyperTerminal). VT-UTF8 is a super-set of VT100 that provides support for block characters, extended PC keyboard keys, colors and non-English output using well-defined escape sequences and UTF8-encoded Unicode as defined in VT-UTF8 specification. All Emergency Management Services (EMS) output is VT-UTF8. The EMS implementation English VT-UTF8 output is backwards compatible with VT100.
Windows Scripting Host	By using Windows Script Host (WSH), you can automate such actions as creating a shortcut and connecting to and disconnecting from a network server. WSH is language independent: you can write scripts in common scripting languages, such as Visual Basic Scripting Edition and JScript.
Automatic Creation of Domain Naming System (DNS) Zone	This feature enables automatic creation of the Domain Name System Zone and configuration of the Domain Name System (DNS) servers running the Windows .NET Server 2003 Family operating system through the enterprise to host this zone. This reduces the time that it would have to take to manually configure every DNS server in the satellite sites to host this zone.

Summary

Building on the foundation established in Windows 2000, Windows .NET Server 2003 will provide a rich set of new features, services, and enhancements. Easier to deploy, configure, and use, Windows .NET Server 2003 will provide centralized, customizable management services to reduce TCO and help users be more productive.

More Information

Microsoft will publish a longer detailed technical overview of this Windows .NET Server 2003 technology on the Web when Release Candidate 1 of Windows .NET Server 2003 becomes available. Link to these longer technical articles at

<http://www.microsoft.com/windows.netserver/techinfo/overview> .

Networking and Communications

Introduction

Networking and communications has never been more critical for organizations faced with the challenge of competing in the global marketplace. Employees need to connect to the network wherever they are and from any device. Partners, vendors, and others outside the network need to interact efficiently with key resources, and security is more important than ever.

Networking improvements and new features in the Windows .NET Server 2003 Family will extend the versatility, manageability, and dependability of network infrastructures, expanding on the foundation established with the Windows 2000 Server family. This section provides an overview of benefits, new features, and improvements for networking and communications services in the Windows .NET Server 2003 Family.

Benefits

In response to continually changing business needs, the Windows .NET Server 2003 Family will provide organizations with the latest standards based networking technologies, delivering the simplified management environment and versatility that businesses demand.

Benefit	Description
Extended Versatility	One of the major challenges facing organizations is responding to varying business requirements—efficiently and effectively. Whether looking to the future of networking or incorporating legacy technologies, the Windows .NET Server 2003 Family is the most versatile network operating system available today. Leading edge technologies such as Internet Protocol version 6 (IPv6) lay the groundwork for the future of networking while support for Point-to-Point Protocol over Ethernet (PPPoE) and Internet Protocol Security (IPSec) Network Address Translator (NAT) traversal respond to the current needs of customers for easy and secure Internet communication.
Increased Dependability	The Windows .NET Server 2003 Family delivers dependability by significantly improving both reliability and security for all wired and wireless scenarios. With the introduction of a basic firewall (Internet Connection Firewall) and new network-access security capabilities using IEEE 802.1X (Extensible Authentication Protocol over LAN) for clients, the Windows .NET Server 2003 Family delivers revolutionary methods for securing access and protecting both wired and wireless networks. Reliability additions include a load balancing capability for both IPSec-based virtual private network (VPN) services as well as Internet Authentication Service (IAS) servers.
Simplified Management	Microsoft continually solicits feedback from customers to help improve our products. Many of the manageability improvements in the Windows .NET Server 2003 Family are attributable to the outstanding suggestions provided by customers. As such, the Windows .NET Server 2003 Family will provide a wider range of features to simplify management duties. These include easier management through Group Policy and updates to the Connection Manager Administration Kit (CMAC) for centralized remote access client deployments.

	The improved Manage Your Server wizard makes it easier than ever to build a dial-up or VPN gateway. Additionally, IAS includes a rich set of new features to simplify network authentication and access control for VPN, dial-up, and IEEE 802.1X-based wired or wireless deployments.
--	---

New Features and Improvements

Windows .NET Server 2003 will provide the following:

- Improved Versatility
- Flexible Manageability
- Robust Dependability

Improved Versatility

The Windows .NET Server 2003 Family will provide the following features for extended versatility.

Feature	Description
Internet Protocol version 6 (IPv6)	IPv6 is the next generation of the Internet layer protocols of the TCP/IP protocol suite. IPv6 solves the current problems of Internet Protocol version 4 (IPv4) with respect to address depletion, security, autoconfiguration, extensibility, and more. The IPv6 protocol provided with the Windows .NET Server 2003 Family includes enhancements to commonly used TCP/IP tools (including Ipconfig, Route, Netstat, Ping, Tracert, and Pathping) and extensive API support (including Windows Sockets, Remote Procedure Call [RPC], and IPHelper). IPv6-enabled system components include Internet Explorer, Telnet client, FTP client, Internet Information Services (IIS) 6.0, file and print sharing, and others. This does not mean that using IPv6 will cause manageability issues with IPv4. The Windows .NET Server 2003 Family provides support for IPv6 and IPv4 coexistence with technologies such as 6to4 and Intra-site Automatic Tunnel Addressing Protocol (ISATAP).
Point-to-Point Protocol over Ethernet (PPPoE)	The Windows .NET Server 2003 Family delivers a native PPPoE driver for making broadband Internet connections without the need for additional software. Small businesses or corporate branch offices may also utilize PPPoE for demand-dial connections using the Routing and Remote Access service.
Network Bridging	Network bridging allows administrators to interconnect separate LAN segments and create a single network segment, also known as a subnet, using computers running a member of the Windows .NET Server 2003 Family. In a multi-LAN segment network, one or more computers may have multiple network adapters such as a wireless adapter, a dial-up adapter, or an Ethernet adapter. Bridging these adapters allows the computers and devices on each of the LAN segments to communicate with each other through the bridge or communicate with the Internet when Internet Connection Sharing (ICS) is enabled on the adapter connected to the Internet.
Internet Protocol Security (IPSec) Network Address	The Windows .NET Server 2003 Family allows IPSec traffic, including Layer Two Tunneling Protocol (L2TP) with IPSec (L2TP/IPSec) connections, to pass through a NAT. This capability is based on the Internet drafts titled "UDP Encapsulation of IPSec

Translator (NAT) Traversal	Packets" (draft-ietf-ipsec-udp-encaps-02.txt) and "Negotiation of NAT-Traversal in the IKE" (draft-ietf-ipsec-nat-t-ike-02.txt).
DHCP with Active Directory and DNS	Dynamic Host Configuration Protocol (DHCP) works with DNS and Active Directory on IP networks, helping to free you from assigning and tracking static IP addresses. DHCP dynamically assigns IP addresses to computers or other resources that are connected to an IP network
Routing and Remote Access	Routing and Remote Access replaces the Routing and Remote Access Service (RRAS) and Remote Access Service (RAS) features from Windows NT 4.0. Routing and Remote Access is a single, integrated service that terminates connections from either dial-up or VPN clients and provides routing (IP, IPX, and AppleTalk). With Routing and Remote Access, your server can function as a remote access server, a VPN server, a LAN router, or a branch-office router.
Preshared Key Authentication for L2TP/IPSec Connections	The Routing and Remote Access service now supports the configuration of a preshared key to authenticate the IPSec portion of an L2TP/IPSec connection. Although not recommended, the preshared key can be used as an interim authentication method while deploying a public key infrastructure (PKI) for certificate-based IPSec authentication.
TAPI 3.1	TAPI 3.1 unifies IP and traditional telephony to enable developers to create computer telephony applications that work as effectively over the Internet or an intranet as they do over the traditional telephone network. TAPI includes enhancements to audio and video streaming in the Windows .NET Server 2003 Family.
Virtual Private Network (VPN)	You can allow secured access to your telecommuters, and mobile workforce by leveraging their connectivity to the Internet even when they are out of the office—thus reducing the cost of access—by implementing a virtual private network (VPN). The VPN connection creates a secure tunnel across the Internet into the private network. VPN also enable corporations to cost effectively connect multiple corporate sites
NetBIOS over TCP/IP (NetBT) Name Resolution Proxy	The NetBT proxy allows a small business to configure a remote access or VPN server so that its employees can work from home. With the NetBT proxy enabled, clients connecting remotely are able to resolve the names of computers on the small business network without requiring the deployment of a DNS or WINS server.
Internet Connection Sharing (ICS)	This feature provides shared Internet connectivity and network services for a home or small business network. ICS provides network address translation functionality, allowing multiple computers on a network to access the Internet at the same time through a dial-up or broadband network connection. Additionally, ICS provides Dynamic Host Configuration Protocol (DHCP) server and Domain Name System (DNS) proxy services for clients on the private network.
IP over IEEE 1394 Support	Support for RFC 2734 allows TCP/IP traffic on an IEEE 1394 serial bus.

Flexible Manageability

The Windows .NET Server 2003 Family will provide the following features for simplified management.

Feature	Description
Additions to Group Policy	New Group Policy improvements in the Windows .NET Server 2003 Family give administrators granular control over most network configuration settings. For example, administrators may now configure some DNS client settings on computers running Windows XP or a member of the Windows .NET Server 2003 Family using Group Policy. This simplifies the steps required to configure domain members when adjusting DNS client settings such as enabling and disabling dynamic registration of the DNS records by the clients, using devolution of the primary DNS suffix during name resolution and populating DNS suffix search lists. Furthermore, the Group Policy feature may be used to allow or restrict user configuration access to individual components of the network user interface (UI).
Connection Manager	Connection Manager provides simplified deployment and configuration for dial-up and VPN remote access connections for an enterprise and for outsourced dial configurations. New Connection Manager features include: • Connection Manager Favorites: This feature enables users to eliminate repetitive configuration of the Connection Manager properties when switching between common dialing locations. • Automatic Proxy: The Automatic Proxy Configuration feature provides the ability to create a Connection Manager profile in order to ensure that the user's computer has appropriate access to both internal and external resources during a connection to a corporate network. • Client Log Files: This feature provides the ability to turn on log files to quickly and accurately troubleshoot problems with Connection Manager connections. • VPN Server Selection: Using the Connection Manager Administration Kit (CMAK), a Connection Manager profile can be created that allows users to select a VPN server to use when connecting to the organization's network. • Preshared Keys: This feature provides a mechanism for automatically distributing a preshared key to remote access clients for use during an L2TP/IPSec VPN connection.
Enhanced Connection Manager Administration Kit (CMAK)	CMAK gives administrators the ability to predefine connection profiles for remote access users running the Windows .NET Server 2003 Family, Windows XP, Windows 2000, Windows NT 4.0, Windows Millennium Edition, and Windows 98. CMAK for the Windows .NET Server 2003 Family allows the configuration of the new features of Connection Manager, as previously described. CMAK has expanded wizard functionality, including improved panes and the ability to perform most advanced customization tasks before building the user profiles. It streamlines the process of building custom client connection packages. This reduces the need to edit .cms or .cmp files for most advanced customization needs. A greater variety of custom actions are available and configurable from within the CMAK Wizard, including custom actions specifically for VPN connections.
Connection Manager: Route Management	The Route Management feature of Connection Manager provides the following: • Enables a network administrator to redirect Internet traffic for VPN connections to avoid use of corporate bandwidth for access to external sites.

	• Predefines routes to the corporate network as part of the Connection Manager profile in order to control access on a per-profile basis. • Includes an option to maintain a routing table at a Uniform Resource Locator (URL). • Allows for a special case in which a network administrator desires both predefined files in the CM profile and additional routes at the same URL.
Internet Authentication Service (IAS) Enhancements	Wireless network deployments dramatically increase demand for multiple RADIUS servers and better tools to diagnose authentication issues and manage network access control. The Windows .NET Server 2003 Family addresses this with new features that allow IAS to send RADIUS logging information to a Structured Query Language (SQL) server to allow advanced SQL queries against network access events across the enterprise, new 802.1X authentication features, cross-forest authentication, and other features. Using IAS, the Windows .NET Server 2003 Family makes it easier to deploy high-scale solutions for authenticated network access control in wired, wireless, and remote access scenarios. To simplify administration of RADIUS clients when there are numerous wireless access points on the same network segment, IAS allows RADIUS clients to be configured by using an address range. IAS now supports the ability to configure specific types of user-level certificates for specific types of connections, based on the certificate Enhanced Key Usage (EKU) object identifiers (OIDs) that must be included in the certificate of the access client. For example, if an IT administrator wanted to ensure that remote access VPN connections use a smart card certificate rather than a locally installed user certificate, they would configure the appropriate remote access policy to require that the object identifier for the Smart Card Logon certificate EKU (1.3.6.1.4.1.311.20.2.2) is present in the certificate offered by the remote access VPN client.
Network Load Balancing Manager	A new Network Load Balancing (NLB) Manager will provide a single point of configuration and management for load balancing.
Alternate Configuration for Multiple Networks	This feature provides the mobile computer user seamless operation when moving between office and home networks without having to manually reconfigure TCP/IP settings. This feature specifies that TCP/IP will use an alternate configuration if a Dynamic Host Configuration Protocol (DHCP) server is not found. The alternate configuration is useful in situations where the computer is used on more than one network and one of those networks does not have a DHCP server and Automatic Private IP Addressing (APIPA) configuration is not desired.
IPSec Command-line Management with Netsh	You can use Netsh commands to configure static or dynamic IPSec main mode settings, quick mode settings, rules, and configuration parameters. The IPSec Netsh commands replace the Ipsecpol.exe tool provided with the Windows 2000 Server Resource Kit. An IT administrator can use this feature to script and automate IPSec configuration.
IP Security Monitoring Improvements	This feature improves IPSec monitoring capabilities with a new IP Security Monitor snap-in that provides detailed IPSec policy configuration and information about the active security state. This feature replaces the Ipsecmon.exe program provided with Windows 2000.

Wireless Monitoring Improvements	The Windows .NET Server 2003 Family includes a new Wireless Monitor snap-in, which can be used to view wireless access point (AP) or wireless client configuration and statistical information.
Wireless Extensions to Group Policy	A new Wireless Network (IEEE 802.11) Policies Group Policy extension allows you to configure wireless network settings that include the list of preferred networks, Wired Equivalent Privacy (WEP) settings, and IEEE 802.1X settings. These new extensions make it much easier to deploy a specific configuration for secure wireless connections to wireless client computers.
Network Location Awareness	This feature allows computers running the Windows .NET Server 2003 Family to detect information about the network to which the computer is attached. Components in the Windows .NET Server 2003 Family use the network location to provide the appropriate services. For example, the new Group Policy settings to enable or disable the Internet Connection Sharing, Internet Connection Firewall, and Network Bridge features are network location-aware; they only apply to the computer when it is connected to the network on which the settings were obtained.
Enhancements to Network Diagnostics	• Network Diagnostics Web page – The Network Diagnostics Web page can be viewed from the Tools section of Help and Support, or the Help and Support detailed information section on either troubleshooting or networking. • Netsh diag commands – New Netsh diag commands enable you to view extensive network diagnostic information and perform diagnostic functions from a command line. • Repair menu option for network connections – A Repair option is available on each network connection's context menu. Choosing this option causes a series of steps to correct the most common networking problems. • Support tab for network connections – The Status dialog box for each network connection in the Network Connections folder now includes a Support tab, on which TCP/IP configuration information is displayed. • Networking tab for Task Manager – Task Manager now includes a Networking tab that displays real time networking metrics for each network adapter in the system. • Updated Netdiag.exe command line network diagnostics tool – The support tools provided on the Windows .NET Server 2003 Family product CD-ROM include Netdiag.exe, an enhanced version of the diagnostics tool provided in the Windows 2000 Resource Kit. • Menu option to enable remote access logging - A new Diagnostics tab has been added to the Remote Access Preferences dialog box in the Network Connections folder to globally enable, view, and clear logging for remote access connections.

Robust Dependability

The Windows .NET Server 2003 Family will provide the following features for increased dependability.

Feature	Description
Internet Connection Firewall (ICF)	The Windows .NET Server 2003 Family introduces Internet security in the form of a firewall. Internet Connection Firewall (ICF), designed for use in a small business, provides basic protection for computers directly connected to the Internet or on LAN segments connected to the Internet.

	ICF is available for LAN, dial-up, VPN, or PPPoE connections. ICF integrates with Internet Connection Sharing (ICS) or with the Routing and Remote Access service.
IPSec Network Load Balancing (NLB)	Network Load Balancing (NLB) provided with the Windows .NET Server 2003 Family now provides support for IPSec traffic. Administrators can use NLB for a group of servers to provide scale-out reliability and capacity for IPSec-protected applications and Windows VPN gateway deployments. For VPN gateways, the NLB improvements support both L2TP VPNs that are protected by IPSec encryption and Point-to-Point Tunneling Protocol (PPTP)-based VPN connections.
Secure Wireless LANs	The Windows .NET Server 2003 Family lets companies move to an “all physical network access is authenticated and encrypted” model through its support of IEEE 802.1X. Using IEEE 802.1X-based wireless access points or switches, companies can be sure that only trusted systems are allowed to connect and exchange frames with secured networks. Because IEEE 802.1X with Extensible Authentication Protocol-Transport Level Security (EAP-TLS) provides dynamic key determination, IEEE 802.11 wireless network security is dramatically improved by addressing many of the known issues associated with WEP and IEEE 802.11-defined authentication). Using the Protected Extensible Authentication Protocol (PEAP), as co-authored by Microsoft in the IETF Internet draft titled "Protected EAP", organizations have the option of using Windows domain passwords for authenticated and encrypted wireless communication without having to deploy a certificate infrastructure and preserving interoperability with any IEEE 802.11 and 802.1X wireless access point. By using the Internet Authentication Service (IAS), companies can also grant Internet access to “guest” users through 802.1X authentication or bootstrap a system configuration in an authenticated network. Administrators may now quarantine connectivity requests that do not submit valid credentials for authentication, isolating the network communications to specific address ranges or a virtual local area network (VLAN), such as the Internet or a bootstrap configuration network segment.
IAS: RADIUS Proxy and Load Balancing	IAS supports RADIUS proxy capabilities, allowing for flexible rule-based forwarding, selective forwarding for authentication and accounting requests to other RADIUS servers, and the ability to force the client to use a compulsory tunnel with or without user authentication. The forwarding capability can be used when connecting users from two-way untrusted forests or domains. IAS proxy support also allows you to load balance RADIUS authentication traffic between multiple IAS servers, providing scalability and geographic failover.
IAS: RADIUS Proxy and Authentication Improvements	This feature provides authentication improvements for wireless, dial-up, and VPN users in other forests, un-trusted domains or other RADIUS user databases. IAS can provide authentication and authorization for user accounts that are members of the domain or forest in which the IAS server is a member. If Active Directory forests are in cross-forest mode with two-way trusts, then IAS as a RADIUS server can authenticate the user account in the other forest. However, If the user account is in another Active Directory forest without cross-forest mode, one-way trusted forest, an un-trusted forest, or in another RADIUS user database, then a RADIUS proxy is needed. IAS as a RADIUS proxy is used to route RADIUS messages between RADIUS servers

	and RADIUS clients. Instead of configuring access servers to send their connection requests to an IAS RADIUS server, they can be configured to send connection requests to an IAS RADIUS proxy. The IAS RADIUS proxy uses the realm name portion of the user name and forwards the request to an IAS server in the correct domain or forest. Connection attempts for user accounts in one domain or forest can be authenticated for network access servers in another domain or forest.
IAS: EAP-TLS Unauthenticated Access	Extensible Authentication Protocol - Transport Level Security (EAP-TLS) unauthenticated access provides a means to grant guest access for a wireless or network switch client that does not have a certificate installed. If a network access client does not provide credentials, IAS determines whether unauthenticated access is enabled in the matching remote access policy. EAP-TLS supports one-way authorization or unauthenticated access where the client does not send credentials. An IT administrator can use this feature to allow wireless or switch clients that do not have certificates to connect to a restricted VLAN to install certificates. An IT administrator can also use this feature to allow access to visitors or business partners to the corporation's network to access the Internet. This is done by giving them access to a restricted VLAN that allows only traffic to and from the Internet.
IAS: EAP Configuration Improvements	With this feature, you can configure a remote access policy to accept multiple EAP types for authentication and you can specify the properties of EAP types on a per-policy basis. This allows you much more flexibility in configuring EAP authentication for wireless and VPN connections.
Better Denial of Service Protection for IKE	The Internet Key Exchange (IKE) protocol, used to negotiate IPSec security associations, has been modified in the Windows .NET Server 2003 Family to better handle denial of service attacks involving IKE traffic.
TCP Receive Window Size Determined by the Local NIC	The window size determines the maximum number of bytes that can be sent without requiring an acknowledgement. On a slower speed dial-up network connection, the window size will be almost equal to the queue depth on the remote access server. When the queue is filled up with packets from one Transmission Control Protocol (TCP) connection, a new TCP connection cannot be established until all these packets are sent out. The TCP slow start algorithm on the new connection makes this situation worse. With this feature, the Quality of Service (QoS) Packet Scheduler on a system with Internet Connection Sharing (ICS) will adjust the window size advertised to match the dial-up network connection speed. This will reduce the queue depth at the remote access server and enable new connections to work better. This feature only applies when ICS is used.
DHCP: UI for Backup and Restore	This Dynamic Host Configuration Protocol (DHCP) snap-in provides new menu items to backup and restore DHCP databases. These items will be present only if the DHCP server is running a member of the Windows .NET Server 2003 Family.
DHCP: Database Netsh Migrations	This feature enables an easier migration of a DHCP database from one server to another if it is exported and imported using the Netsh tool. This eliminates most manual configurations, such as manually editing the registry or recreating scopes. Netsh is used to configure network services and protocols for local and remote computers and can execute script files to automate configuration tasks.

DNS Enhancements	The Domain Name System (DNS) includes several enhancements and improvements in the Windows .NET Server 2003 Family, including: • Active Directory Integrated DNS Zones Stored in Application Partitions: This feature enables storage and replication of the DNS zones stored in the Active Directory in the application partition. • DNS Security Extensions Compliance: A DNS server running a member of the Windows .NET Server 2003 Family provides basic compliance with the Internet Engineering Task Force (IETF) standard DNS Security Extensions protocol as defined in RFC 2535. • Domain Join Procedure Enhancements to Detect Incorrectly Configured DNS: This feature simplifies debugging and reporting of an incorrect DNS configuration and helps to properly configure the DNS infrastructure required to enable a computer to join a domain. • Stub Zones and Conditional Forwarding: The conditional forwarding feature in Windows .NET Server 2003 Family provides improved granularity supporting name-dependent forwarding. For example, a DNS server may be configured to simultaneously forward queries for names ending in usa.microsoft.com to a first set of DNS servers, forward queries for names ending in europe.microsoft.com to a second set of DNS servers, and forward all other queries to a third set of DNS servers. • Support for EDNS0 Protocol: The Windows .NET Server 2003 Family provides support for this IETF standard protocol as defined in RFC 2671. This feature allows DNS servers to accept and transmit User Datagram Protocol (UDP) DNS messages with a payload size greater than 512 octets.
-------------------------	---

Summary

Building on the foundation established in the Windows 2000 Server family, the Windows .NET Server 2003 Family will deliver new networking features and improvements ensuring that it is one of the most flexible operating systems in the marketplace today.

More Information

Microsoft will publish a longer detailed technical overview of this Windows .NET Server 2003 technology on the Web when Release Candidate 1 of Windows .NET Server 2003 becomes available. Link to these longer technical articles at <http://www.microsoft.com/windows.netserver/techinfo/overview> .

Security

Introduction

Businesses have extended the traditional local area network (LAN) by combining intranets, extranets and Internet sites; as a result, increased system security is now more critical than ever before. To provide a secure computing environment, the Windows .NET Server 2003 operating system will provide many important new security features and improves on the security features originally included in Windows 2000 Server.

Trustworthy Computing

Viruses exist and software security is an ongoing challenge. To address these facts Microsoft has made Trustworthy Computing a key initiative for all its products. Trustworthy Computing is a framework for developing devices powered by computers and software that are as secure and trustworthy as the everyday devices and appliances you use at home. The basic redesign of Windows .NET Server 2003 is a solid step towards making this vision a reality.

The Common Language Runtime

The Common Language Runtime (CLR) software engine is a key element of Windows .NET Server 2003 that improves reliability and helps ensure a safe computing environment. It reduces the number of bugs and security holes caused by common programming mistakes—as a result, there are fewer vulnerabilities for attackers to exploit.

CLR verifies that applications can run without error and checks for appropriate security permissions; making sure that code only performs appropriate operations. It does this by checking for things such as: where the code was downloaded or installed from; whether it has a digital signature from a trusted developer; and whether the code has been altered since it was digitally signed.

Benefits

Windows .NET Server 2003 will provide a more secure and economical platform for doing business

Benefit	Description
Lower Costs	This results from simplified security management processes such as access control lists and Credential Manager.
Implementation of Open Standards	The IEEE 802.1X protocol makes it easy to secure wireless LANs from the threat of eavesdropping within your business environment.
Protection for Mobile Computers and other New Devices	Security features such as Encrypting File System (EFS), certificate services, and automatic smart card enrollment make it easier to secure a full range of devices. EFS is the core technology for encrypting and decrypting files stored on NTFS volumes. Only the user who encrypts a protected file can open the file and work with it. Certificate Services is the part of the core operating system that allows a business to act as its own certification authority (CA) and issue and manage digital certificates. Automatic smart card enrollment and self-registration authority features provide enhanced security for enterprise users by adding another layer of authentication; this is in addition to simplified security processes for security conscious organizations.

New Features and Improvements

The Windows .NET Server 2003 Family will provide the following:

- A more secure platform for doing business.
- The best platform for your public key infrastructure.
- Secure extension of your business to the Internet.

A More Secure Platform for Doing Business

Windows .NET Server 2003 will provide many new and improved features that combine to create a more secure platform for doing business.

Feature	Description
Internet Connection Firewall (ICF)	The Windows .NET Server 2003 Family will provide Internet security using a software-based firewall called Internet Connection Firewall (ICF). ICF provides protection to computers directly connected to the Internet. ICF is available for LAN, dial-up, VPN, or PPPoE connections. ICF integrates with Internet Connection Sharing (ICS) or with the Routing and Remote Access service.
Internet Authentication Service (IAS) RADIUS Server and Proxy	The Internet Authentication Service (IAS) is a Remote Authentication Dial-in User Service (RADIUS) server and proxy that manages user authentication and authorization. As a RADIUS server, it provides authentication, authorization, and accounting for network access such as dial-up, virtual private networks (VPNs), and IEEE 802.1X-based wired and wireless connections.
Secure Wireless and Ethernet LANs	The Windows .NET Server 2003 Family lets companies move to an “all physical network access is authenticated and encrypted” model through its support of IEEE 802.1X. Using IEEE 802.1X-based wireless access points or switches, companies can be sure that only trusted systems are allowed to connect and exchange packets with secured networks. Because IEEE 802.1X with Extensible Authentication Protocol-Transport Level Security (EAP-TLS) provides dynamic key determination, IEEE 802.11 wireless network security is dramatically improved by addressing many of the known issues associated with IEEE 802.11-defined authentication and Wired Equivalent Privacy (WEP). Using the Protected Extensible Authentication Protocol (PEAP), as co-authored by Microsoft in the IETF Internet draft titled “Protected EAP”, organizations have the option of using Windows domain passwords for authenticated and encrypted wireless communication without having to deploy a certificate infrastructure, while preserving interoperability with any IEEE 802.11 and 802.1X wireless access point. By using Internet Authentication Server (IAS), companies can also grant Internet access to “guest” users through 802.1X authentication or bootstrap a system configuration in an authenticated network. Administrators may now quarantine connectivity requests that do not submit valid credentials for authentication, isolating the network communications to specific address ranges or a virtual local area network (VLAN), such as the Internet or a bootstrap configuration network segment.
Software Restriction Policies	This feature provides a policy-driven mechanism to identify software running in a domain and control its ability to execute. It can identify software that is hostile or unwanted and prevent it from executing on computers running Windows XP and Windows .NET Server 2003 Family. This allows you to improve management of computers running Windows XP and Windows .NET Server 2003 Family in a way that

	allows better defenses against viruses, Trojans and unwanted applications. This feature also allows you to limit the software that runs on highly managed workstations (such as kiosks, task stations, or application stations) to only a certain list of software. This can help improve system stability and integrity for these computers. This feature is run from the Manage Group Policy snap-in.
Increased Web Server Security	Information security is a critically important issue for organizations everywhere. To increase Web server security, Internet Information Services 6.0 (IIS 6.0) will be configured for maximum security right out of the box—its default installation is "locked down." Advanced security features in IIS 6.0 include: selectable cryptographic services, advanced digest authentication, and configurable access control of processes. These are among the many new security features that enable you to conduct business securely on the Web.
Encrypting the Offline Files Database	The option to encrypt the Offline Files database is now available. This is an improvement over Windows 2000 where cached files could not be encrypted. Administrative privileges are required to configure how offline files will be encrypted.
FIPS-compliant, Kernel-mode, Crypto Module	This cryptographic module runs as a driver in kernel-mode and implements Federal Information Processing Standard (FIPS)-approved cryptographic algorithms. These algorithms include: SHA-1, DES, 3DES, and an approved random number generator. The FIPS-compliant, kernel-mode, crypto module lets governmental organizations deploy FIPS 140-1-compliant, Internet Protocol Security (IPSec) implementations using: • Layer Two Tunneling Protocol (L2TP)/IPSec VPN client and server. • L2TP/IPSec tunnels for router-to-router (also known as gateway-to-gateway) VPN connections. • IPSec tunnels for gateway-to-gateway VPN connections. • IPSec-encrypted, end-to-end, network traffic between client and server, and server to server.
New Digest Security Package	The new digest security package supports the digest authentication protocol, along with RFC 2617 and RFC 2222. These protocols are supported by both Microsoft Internet Information Services (IIS) and the Active Directory service. Advanced Digest Authentication, based on Internet Engineering Task Force (IETF) RFC 2617, behaves the same as Digest Authentication except for the way in which user credentials are stored on the Domain Controller (DC). Advanced Digest Authentication is a security improvement over Digest Authentication. Digest Authentication only sends users credentials across the network as an MD5 hash. Advanced Digest Authentication also does this plus it also stores user credentials in Active Directory on the DC as an MD5 hash, also known as a message digest. Due to this improvement, unauthorized access to the DC cannot feasibly discover passwords of users. Advanced Digest Authentication is available to Web Distributed Authoring and Versioning (WebDAV) directories. It does not replace Digest Authentication. Using Advanced Digest Authentication also provides improved security because credentials do not have to be stored in reversible encryption on the DC, delegated digest works over Proxy servers, delegated digest is lightweight, there is no additional client software required and usernames and passwords are not passed in clear text over the Internet.
System Security Improvements	Important improvements have been made to ensure overall system security including: • Increased performance improvement of over 35 percent when using the secure

	sockets layer (SSL). IIS is not installed by default. To deploy IIS, it first has to be installed using Add/Remove Programs in the Control Panel. Buffer checking capability in Microsoft Visual Studio®. (Buffer overruns are commonly used by hackers to exploit a system.)
Credential Manager	Credential Manager in Windows .NET Server 2003 will provide a secure store for user credentials, including passwords and X.509 certificates. These credentials provide a consistent, single sign-on experience for users—including roaming users. A Win32 API is available that allows server- and client-based applications to obtain user credentials.
SSL Client Authentication Improvements	In Windows .NET Server 2003 the SSL session cache can be shared by multiple processes. This reduces the number of times a user has to reauthenticate with applications, and reduces CPU cycles on the application server.
Kerberos V5 Support	Kerberos V5 is a mature, industry-standard network authentication protocol. With Kerberos V5 support, a fast, single logon process gives users the access they need to enterprise resources, as well as to other environments that support this protocol. Support for Kerberos V5 includes additional benefits, such as mutual authentication (client and server must both provide authentication) and delegated authentication (the user's credentials are tracked end to end).
Easy Trust Creation	This feature includes three key elements: - A new Trust Wizard is provided to create both sides of trust link in one operation if proper credentials are supplied for both sides of the trust. This applies to Windows 2000 and Windows .NET Server 2003 Family and is for external or forest trust links. - A new Trust API is also provided to support delegation required to deploy Resource Forests. This includes matching credentials required to type of trust so domain users can create inbound Forest trust and enforce quotas on user create Trust links. - A version control tools updates system parameters when a Windows 2000 domain or forest is upgraded to the Windows .NET Server 2003 Family operating system. This includes parameters such as version levels, schema changes, and default Access Control Lists (ACLs).

The Best Platform for Your Public Key Infrastructure

Windows .NET Server 2003 will make it easier to deploy a public key infrastructure, along with associated technologies like smart cards.

Feature	Description
Certificate Services	Using Certificate Services and certificate management tools, you can deploy your own public key infrastructure. With a public key infrastructure, you can implement standards-based technologies, such as smart card logon capabilities, client authentication (through Secure Sockets Layer and Transport Layer Security), secure e-mail, digital signatures, and secure connectivity (using Internet Protocol security (IPSec)). Using Certificate Services, you can set up and manage certification authorities that issue and revoke X.509 V3 certificates. This means that you do not have to depend on commercial client authentication services, although you can integrate commercial client authentication into

	your public key infrastructure if you choose. Among the Enhancements available in Windows .NET Server 2003 are: • Enrollment Enhancements: This feature will enable applications to expect the existence of certificates without the need to develop alternative enrollment processes. This is intended to make it easier for users to deal with certificates. This feature includes user auto-enrollment, user auto-renewal, delegated enrollment, and manual certificate requests. • Certificate Mapping: This feature allows Active Directory Issuer-only (Many-To-One) Client Certificate mapping through Secure Sockets Layer/Transport Layer Security (SSL/TLS) based on any Subordinate Certificate Authority in the certificate chain. Note: In previous versions of Windows, it was only possible to do Many-To-One mapping based on the direct issuer of the end certificates. • Editable Certificate Templates: This feature provides the capability to edit a Certificate template. It also includes changes to meet the X.509 standard to include deployment specific information in the certificates and certificate templates.
Smart Card Infrastructure	Using Certificate Services and certificate management tools, you can deploy your own public key infrastructure. With a public key infrastructure, you can implement standards-based technologies, such as smart card logon capabilities, client authentication (through Secure Sockets Layer and Transport Layer Security), secure e-mail, digital signatures, and secure connectivity (using Internet Protocol security (IPSec)). This feature improves the tools for expanded use of Smart Card technology. These improvements include DCPromo, "Run As", "Map Network Drive", command line "run as" and net.exe. In addition, the Credential Management User Interface (UI) is improved to support 'smart' credential collection including retrieval of logon certificates from Smart Cards. It will also be modified to provide support for simple command line UI to collect Smart Card credentials for the command line tools.
Certificate Autoenrollment and Autorenewal	These important new features dramatically reduce the amount of resources needed to manage X.509 certificates. Windows .NET Server 2003 will make it possible to automatically enroll and deploy certificates to users—and as certificates expire, they can be automatically renewed. Certificate autoenrollment and autorenewal make it easier to deploy smart cards faster, and improve the security of wireless (IEEE 802.1X) connections by automatically expiring and renewing certificates.
Windows Installer Digital Signature Support	Digital signature support enables Windows Installer packages and external cabinets to be digitally signed. This lets IT administrators provide a more secure Windows Installer package, which is especially important if a package is sent over the Internet. This also allows Windows Installer Packages to honor the new Software Restriction policy settings for specifying what applications can be used.
Certificate Revocation List (CRL) Improvements	The certificate server included in Windows.NET Server now supports delta Certificate Revocation Lists (CRLs). A CRL makes the publication of revoked X.509 certificates more efficient, and makes it easier for a user to retrieve a new certificate. And because you can now specify the location where a CRL will be stored, it's much easier to move it to accommodate specific business and security needs.

Key Archival and Recovery	Key archival and recovery enables private key management and recovery in the event of end-entity losses. Key Archival and Recovery includes the following features: • Key archival and recovery requires only one recovery agent to recover a private key. • Exposes C-language Application Programming Interfaces (APIs) and one Common Object Model (COM) object interface for external developers to use. • Key archiving is supported only for enterprise Certificate Authorities (CA) with servers running Windows .NET Server 2003 Family. • Key archival is the same for users, computers, and applications. The process of performing a certificate enrollment will be performed without interaction from a user or administrator. • Key recovery involves interaction with a designated recovery agent in a similar manner to how an Encrypted File System (EFS) requires a recovery agent to recover a file encryption key. • Migration from Exchange 2000 KMS and the Outlook® *.epf key storage format will be supported. • Foreign key escrow from third-party Certificate Authorities will be supported.
----------------------------------	--

Secure Extension of Your Business to the Internet

A business needs a secure way to communicate with employees, customers and partners that are not located within its intranet. Windows .NET Server 2003 will make it easier to securely extend access to your network for individuals and other businesses that need to work with data or use resources.

Feature	Description
Passport Integration	A Passport identity can be mapped to an Active Directory identity within Windows .NET Server 2003. For example, by associating a Passport identity with an Active Directory identity a business partner can be authorized to access resources through IIS, rather than having to log on directly to a Windows network. Passport integration will provide an equivalent single sign-on experience using IIS. This feature provides integration of Passport as a supported authentication mechanism for Internet Information Services (IIS). This integration provides Passport authentication in the core Web server and uses Passport version 2 interfaces provided by standard Passport components. After Passport authentication is verified, the Passport user is mapped to an Active Directory user by their Passport Identification if such a mapping exists. A token is created by the Local Security Authority (LSA) for the user and set by IIS for the Hyper Text Transport Protocol (HTTP) request. Application developers and Web site administrators can use this security model for authorization based on Active Directory users and Access Control Lists (ACLs) on servers running IIS services.
Cross-Forest Trusts	If you're working with a partner or company that has an Active Directory forest deployed, you can use Windows .NET Server 2003 to set up a cross-forest trust between their forest and yours. This allows you to explicitly trust certain, or all, users or groups in the other forest. You also have the capability to set permissions based on user or groups that are resident in the other forest. Cross-forest trusts make it easy to conduct business with other

	companies using Active Directory. Additional security features make it easier to manage the multiple forests and cross domain trusts. A new credential manager provides a secure store of user credentials and X.509 certificates. In addition, Forest trust provides a new type of Windows trust for managing the security relationship between two forests—greatly simplifying cross-forest security administration and authentication. Users can securely access resources in other forests, using either Kerberos or NTLM, without sacrificing the single sign-on and administrative benefits of having only one user ID and password maintained in the user's home forest.
Stronger Diffie-Hellman Group for Internet Key Exchange (IKE)	IPSec now supports the use of a 2048-bit Diffie-Hellman key exchange, providing support for the Internet draft titled "More MODP Diffie-Hellman groups for IKE." With a stronger Diffie-Hellman group, the resulting secret key derived from the Diffie-Hellman exchange has greater strength.
Delegation Model Improvements	Delegation model improvements includes improvements to allow any Internet protocol to be used between the client and Web server and then allows the use of Kerberos between the Web server and the back-end data servers. It also includes a new model for Kerberos-based delegation that does not require forward-able Ticket Granting Tickets (TGTs) and enforces constraints on delegation that allow a particular account to delegate only to specific services configured at the domain policy level.

Summary

Efficient and secure networked computing is more important than ever for a business to remain competitive. Windows .NET Server 2003 will let you take advantage of your existing IT investments, and extend those advantages to your partners, customers, and suppliers by deploying key features like cross-forest trusts and Passport integration.

Windows .NET Server 2003 will provide services that create a more secure environment for doing business. It's easy to encrypt sensitive data and software restriction policies can be used to prevent damage caused by viruses and trojans. And Windows .NET Server 2003 is the best choice for deploying a public key infrastructure; its autoenrollment and autorenewal features make it easy to deploy smart cards and certificates across the enterprise.

Getting Secure and Staying Secure

Microsoft is committed to doing what's necessary to help customers get secure and stay secure. The single best thing you can do to maintain the health and security of the computers in your organization is to stay current with the latest security updates as they're made available.

[Subscribe to the Microsoft Security Notification Service](#)

This is a free e-mail notification service that provides accurate information to keep you informed about, and protected from, malicious attacks.

You can also read security bulletins and other information about Microsoft product security on <http://www.microsoft.com/technet/security>.

More Information

Microsoft will publish a longer detailed technical overview of this Windows .NET Server 2003 technology on the Web when Release Candidate 1 of Windows .NET Server 2003 becomes available.

Link to these longer technical articles at

<http://www.microsoft.com/windows.netserver/techinfo/overview> .

Storage Management

Introduction

Windows .NET Server 2003 will introduce new and enhanced features for storage management, making it easier and more reliable to manage and maintain disks and volumes, backup and restore data, and connect to Storage Area Networks (SANs). This section provides an overview of benefits, new features, and improvements for storage management services in Windows .NET Server 2003.

Benefits

Improvements in the operating system help reduce total cost of ownership (TCO), strengthening Windows as a mission-critical platform.

Benefit	Description
Lower TCO for Managing Storage	A primary cost component for businesses today is managing disks and storage. Windows .NET Server 2003 significantly reduces the complexity of managing storage through improved disk management tools and utilities, faster and more reliable disk performance, and new features for network-attached storage. Easy-to-configure file shares through Distributed File Service (DFS) technology make managing and configuring network storage both more reliable and cost-effective.
Lower TCO Through Increased Availability	Another crucial component of TCO is availability: keeping mission critical and customer-facing applications online. Through improved data management, clustering, and disaster-recovery technologies, Windows .NET Server 2003 reduces the number of hours required for planned downtime. Fewer outages and reduced maintenance result in lower costs. More consistent and reliable backup and restore operations mean fewer hours spent administering backups and reduced risk of data loss during restore. In addition, Windows backup has been tailored to meet the needs of smaller businesses relying on lower cost and more reliable backup scenarios, where backup and restore needs to "just work". Support costs are also reduced, as users are empowered to self-maintain or "undelete" accidentally lost or deleted files with new Shadow Copy technology.

New Features and Improvements

Windows .NET Server 2003 will provide an integrated set of storage management features reducing costs and increasing availability.

Feature	Description
Shadow Copies for Administrators	A Volume Shadow Copy of a storage volume is a point-in-time copy of the original entity. The Volume Shadow Copy is typically used by a backup application so that it can backup files that are made to appear static, even though they are really changing. Windows lets administrators configure shadow copies from either the Disk Management Snap-in or the Shared Folders Snap-in, both located in the Computer Management console. When enabled, users can find previous versions of files available from network shares. Volume Shadow Copy features include:

	• Backup and restore files at the file level, the volume level, or the application level • Application Programming Interface (API) that uses the Common Object Model (COM) infrastructure for much of its registration and configuration needs • COM-based "coordinator" service that driver messages between parties involved in the snapshot process and also performs discovery of applications and snapshot providers • Storage filter driver that implements Volume Shadow Copy using a copy-on-write design • Interfaces to support ISV/IHV plug-ins of other Volume Shadow Copies • Interfaces for applications and stores to ensure these Volume Shadow Copies are of consistent state
Shadow Copies for Users	After the shadow copies features are enabled on the server or network share, users can find previous versions of files in Windows Explorer by simply right-clicking the file and selecting Properties.
Encrypting File System (EFS)	The Encrypting File System is the technology used to store encrypted files on NTFS volumes. Encrypted files and folders are easy to use as they appear just like any other file or folder—transparent to authorized users but inaccessible to anyone else. EFS is particularly beneficial for mobile users who may face a higher risk of computer loss or theft. An unauthorized person who tries to access encrypted files or folders is prevented from doing so, even if the intruder has physical access to the computer. EFS improvements in Windows .NET Server 2003 include the ability to authorize additional users to access encrypted files, the ability to encrypt offline files, the ability store encrypted files in Web folders as well as improved encryption methods (3DES).
Open File Backup	The backup utility included with Windows .NET Server 2003 now supports "open file backup". In Windows 2000, files had to be closed before initiating backup operations. Backup now uses Shadow Copies to ensure that any open files being accessed by users are also backed up.
Improved Check Disk (CHKDSK) Command	In Windows .NET Server 2003, the performance of chkdsk.exe is seven times faster than the version released with Windows 2000. The program, which checks for errors on Windows volumes (FAT or NTFS file systems), also provides improved reliability and error-handling capabilities to ensure the program only runs when serious errors occur, or when initiated by the user from the command-line. CHKDSK for Windows .NET Server 2003 will also be available for Windows 2000 Server.
Boot from SAN Configuration	Storage hardware vendors are now making it possible to boot and run a Windows .NET Server 2003 operating system, remotely. SAN boot also requires a custom configuration, depending on your storage hardware vendor. Contact your storage vendor for more information on SAN boot support. In the new Storage Area Network (SAN) technology, all of the disks in a cluster may be in the same storage fabric accessed through a single Host Bus Adapter (HBA). This feature allows all disks (except the boot disk, the system disk and disks containing page files) to be considered as shared disks regardless of the storage bus technology. This feature allows all server storage to be centralized into a SAN including boot, pagefile and system disks using a single or multiple redundant HBAs.
Storage Area	The new Storage Area Network (SAN) technology is viewed as a method to provide data

Network (SAN) Device Arbitration	consolidation and ease of management. Bus reset, a disruptive action for nodes that share a SAN, is not a defined operation. This feature modifies the cluster arbitration mechanism in order to avoid bus resets where possible. The mechanism will try various options before the last alternative of a bus reset.
Automated System Recovery (ASR)	A new feature in Windows .NET Server 2003, Automated System Recovery (ASR) improves productivity by enabling a one-step restore of operating system, system state, and hardware configuration in disaster recovery situations. Automated System Recovery (ASR) feature provides the ability to save and restore applications. This feature also provides the Plug and Play mechanism required by ASR to back up Plug and Play portions of the registry and restore that information to the registry. The backup application included with Windows can be easily configured to use ASR for system restores. Combined with Remote Installation Services (RIS), ASR provides an effective way to automate complete system restores across the network without user intervention. Automated System Recovery (ASR) enables: • Storage Managers to restore entire systems and hardware configurations flexibly • Storage Managers to standardize recovery of Windows operations • ISVs to use for 3rd-party backup products
Virtual Disk Service	A new service in Windows .NET Server 2003, Virtual Disk Service (VDS) provides a single interface for managing block storage virtualization. The service provides for the management of logical volumes (in software) and logical units (in hardware). Management operations include binding, topology discovery and tracking, volume status and fault tracking, and performance tracking. Microsoft Management Console (MMC) Snap-in, Disk Manager and Diskpart command line interface use the new service.
Disk Management Improvements	The Management Console (MMC) Snap-in, Disk Manager has been enhanced to use the new Virtual Disk Service to standardize all disk management operations using the new service to lower TCO through increased availability.
Diskpart Command	The diskpart.exe command-line program provides all the functionality of the Microsoft Management Console (MMC) Snap-in, Disk Manager, and provides additional command operations and scripting functionality for IT professionals to standardize storage configurations and easily recreate storage configurations for business recovery and restore operations. Diskpart has been enhanced to use the new Virtual Disk Service to standardize all disk management operations using the new service. In addition, diskpart enables storage administrators to expand basic disks, a disk type used by Microsoft Cluster Services, as more disk space is required.
DFS Improvements	The Distributed File Service (DFS) eases locating and managing data on your network. DFS provides unified management and access of distributed servers across the Enterprise. DFS unites files on different computers, making them appear to be a single "namespace", enabling a single, hierarchical view of multiple file servers and file server shares on your network. Improvements in DFS deliver more reliable load-balancing, better file replication between DFS sites and servers, and closest-site selection for users accessing the network. Closest-site selection ensures that users share files from the server closest to their network access point. In addition, a single Windows .NET Server 2003 system can host multiple DFS roots. This reduces the administrative and hardware costs associated with managing multiple

	namespaces and multiple replicated namespaces.
Distributed File Service (DFS) Administration Improvements	This feature exposes more functionality of the File Replication Service (FRS) through a new Distributed File Service (DFS) Microsoft Management Console (MMC) Snap-in. Actions supported by this console include: • Removal of replication filtering • Ability to display all types of FRS configurations • Ability to change non-SYSVOL types of FRS configurations • Definition of FRS replica set • Creation of topologies such as full mesh, star and hub • Ability to specify schedule on individual connections • Ability to extend other MMC Snap-ins
DFS File Replication Services (FRS)	File Replication Services (FRS) works in conjunction with DFS by replicating data on file shares, automatically maintaining synchronization between copies across multiple servers. A new feature in Windows .NET Server 2003, the DFS MMC UI allows configuration of replication topologies. The FRS service itself also has new features—compression of replication traffic and the ability to damp unnecessary replication traffic.
Disk Quota	You can use disk quotas on volumes that are formatted with the NTFS file system to monitor and limit the amount of disk space that is available to individual users. You can define the responses that result when users exceed your specified thresholds.
FAT32 on DVD-RAM	This feature enables recognition, mounting, and formatting of 32-bit File Allocation Table (FAT32) volumes on Digital Video Disk-Random Access Memory (DVD-RAM) disks in super-floppy format.
Winsock Direct	Winsock Direct, now available on all Server editions, enables applications that use Winsock to perform faster and with less overhead when they communicate across a system area network (SAN). If there is a SAN in place, Winsock Direct has the effect of streamlining communications between distributed components.
Logical Volume Management Enhancements	Logical Volume Management (LVM) is a function that provides a mapping layer between the disk driver and the file system. This feature is a collection of enhancements that improves performance or availability of storage and file systems. Logical Volume Management enables: • Adding volumes online without reboot • Converting volumes from basic to dynamic • Online growth of volumes without reboot

Summary

New and improved storage management features will make Windows .NET Server 2003 easier to manage, more reliable, and more available. More efficient backup and restore operations combined with good operational practices result in lower TCO and greater customer Return On Investment.

More Information

Microsoft will publish a longer detailed technical overview of this Windows .NET Server 2003 technology on the Web when Release Candidate 1 of Windows .NET Server 2003 becomes available.

Link to these longer technical articles at

<http://www.microsoft.com/windows.netserver/techinfo/overview> .

Terminal Services

Introduction

Microsoft Terminal Services, part of Microsoft Windows .NET Server 2003, builds on the solid foundation provided by the application server mode in Windows 2000 Terminal Services. Terminal Services lets you deliver Windows-based applications, or the Windows desktop itself, to virtually any computing device—including those that cannot run Windows.

Terminal Services in Windows .NET Server 2003 can enhance an enterprise's software deployment capabilities for a variety of scenarios that remain difficult to solve using traditional application distribution technologies. When users run an application on Windows .NET Server 2003 using Terminal Services, the application execution takes place on the server, and only keyboard, mouse and display information is transmitted over the network. Users see only their own individual sessions, which are managed transparently by the Windows server operating system, and remain independent of any other client session.

Windows 2000 Terminal Services remote administration mode is called "Remote Desktop for Administration" in Windows .NET Server 2003, and it supports the Remote Desktop Protocol (RDP) 5.1 feature set. It also has the ability to remote the actual console session of the server.

Benefits

Terminal Services in Windows .NET Server 2003 provides three important benefits.

Benefit	Description
Rapid, Centralized Deployment of Applications	Terminal Services is great for rapidly deploying Windows-based applications to computing devices across an enterprise—especially applications that are frequently updated, infrequently used, or hard to manage. When an application is managed on Terminal Services, and not on each device, administrators can be certain that users are running the latest version of the application.
Low-bandwidth Access to Data	Terminal Services considerably reduces the amount of network bandwidth required to access data remotely. Using Terminal Services to run an application over bandwidth-constrained connections, such as dial-up or shared WAN links, is very effective for remotely accessing and manipulating large amounts of data because only a screen view of the data is transmitted, rather than the data itself.
Windows Anywhere	Terminal Services helps users become more productive by enabling access to current applications on any device—including under-powered hardware and non-Windows desktops. And because Terminal Services lets you use Windows anywhere, you can take advantage of extra processing capabilities from newer, lighter-weight devices such as the Pocket PC.

New Features and Improvements

Terminal Services is the foundation for building an enterprise-wide, server-based computing platform, and includes significant enhancements in Windows .NET Server 2003.

Feature	Description
Increased Scalability	Enterprises need the ability to scale-up and scale-out. Terminal Services in Windows .NET Server 2003 supports more users on each high-end server than Windows 2000; and Session Directory in Enterprise Edition provides support for Microsoft's network load balancing and other third-party load balancing technologies.
Improved Manageability	Terminal Services provides unsurpassed remote manageability by taking advantage of technologies like Group Policy. Complete remote management capabilities are available through a comprehensive read/write Windows Management Instrumentation (WMI) provider.
Easy-to-use Remote Desktop Connection	Remote Desktop Connection (the new "Terminal Services Client") is an RDP 5.1 client that features a much improved user interface, enabling users to save connection settings, easily switch between windowed and full screen mode, and to dynamically alter their remote experience to match the available bandwidth. Remote Desktop provides access to a desktop from any Terminal Services client. This allows access to the full set of installed applications, work in progress, and all connectivity usually found from a workstation or a server. Remote Desktop is an extension of Windows 2000 Terminal Services functionality. It will still allow access to sessions on a computer running Server products that can be used for computer administration or server-based computing. In addition, Remote Desktop allows Remote Console access, allowing one to redirect the primary screen output to a Terminal Services client. APIs are available that allow an application to determine if it is running on the local console or as a Remote Desktop. Additional Terminal Services APIs provide general session information. The Remote Desktop Connection is the end-user tool for establishing connections to computers running Terminal Services. It is now included in all product platforms. Remote Desktop Connection replaces the Terminal Services Client.
Enhanced Remote Desktop Protocol (RDP)	When connecting to Terminal Services in Windows .NET Server 2003 using an RDP 5.1 client, many of the local resources are available within the remote session, including the client file system, smart cards, audio (output), serial ports, printers (including network), and the clipboard. These redirection facilities allow users to easily take advantage of the capabilities of their client device from within the remote session. For instance, files can be opened, saved and printed to the users local PC, regardless of whether the application is running locally or remotely.
Greater Color Depth and Screen Resolution	With RDP 5.1, color depth can be selected from 256 colors (8-bit) to True Color (24-bit), and resolution can be set from 640 x 480 up to 1600 x 1200. For example, an IT administrator can use Terminal Services to support store kiosks displaying merchandise. They can be set to provide true color images for the best product image.

Load Management	Session-based and server-based load management is available for Terminal Services. Server load management uses Windows Management Instrumentation (WMI) to provide metrics to network or hardware load balancing services. These metrics provide information on server availability and load, including server up, server down, and number of additional sessions the server can support. The load balancer or router can then use this data to better control server use. Session load management provides a Session Directory facility to re-route disconnected users back to their session in progress. The Session Directory is a replaceable Common Object Model (COM) object.
Remote Connection Permissions	Terminal Services introduces the Remote Desktop Users group, a new mechanism for granting users remote access to a computer for administration, Remote Desktop connection, or application sharing with Terminal Services. Remote Desktop Users is a built-in group that can be administered through policy. Placing a user or group into Remote Desktop Users gives that user the ability to remotely connect to a computer. The user does not also need to be given local log-in privileges, as in earlier versions of Terminal Services. Local users also do not need to be given separate remote access permissions. By default, the Remote Desktop Users Group includes the same entries as the User group for true Terminal Services (previously known as application-server mode), but it is empty otherwise on all non-application-server configurations, and when a new user is added to Users this is automatically added to Remote Desktop Users. The user may also be removed if desired. On an upgrade from Windows 2000, if there were no special configurations set in the Permissions through Terminal Services Configuration, this same paradigm is followed. If the Security Descriptor (SD) has users explicitly listed, then no attempt is made to move users to the remote-desktop group because each item (user) might have had special Terminal Services permissions masks different than the default permissions masks given to the Remote Desktop User group. The only modification made to the SD is to insert the Remote Desktop User group in the SD list. The Permissions tab in Terminal Services Configuration can still be used to add specific users, as it was in Windows 2000, or to set particular permissions for users. However, users must be granted the Remote Interactive Logon right to be able create a remote Terminal Services connection. This Logon right may be given to any user or group using the Security policy editor, SecPol.MSC, or by simply adding that user or group to the Remote Desktop Users group. If there are multiple connections to Terminal Services in a Windows .NET Server 2003, and an administrator wants to configure user permissions differently for each Network Interface Card (NIC), a combination of the Remote Desktop Users group and the Permissions tab (or Windows Management Instrumentation, WMI, Permissions functionality) will provide this. Typically, Remote Desktop Users would be removed from all configurations, all users or user groups who should have access to the computer are put into Remote Desktop Users, and the particular users or groups who should have access by using a particular NIC are put into that permission set.
Leverages Windows .NET Server 2003 Enhancements	Terminal Services takes advantage of many Windows .NET Server 2003 features, such as software restriction policies, roaming profile enhancements, and new application compatibility modes.

Summary

Terminal Services in Windows .NET Server 2003 builds on the foundation of Windows 2000 Terminal Services by providing organizations with a more reliable, more scalable, and more manageable server-based computing platform. Terminal Services offers new options for application deployment, more efficient access to data over low bandwidth, and enhances the value of legacy and new, lighter-weight devices. Whether using third-party add-ons or not, administrators and users will appreciate the new capabilities that will be delivered by Terminal Services in Windows .NET Server 2003.

More Information

Microsoft will publish a longer detailed technical overview of this Windows .NET Server 2003 technology on the Web when Release Candidate 1 of Windows .NET Server 2003 becomes available.

Link to these longer technical articles at

<http://www.microsoft.com/windows.netserver/techinfo/overview> .

Enterprise UDDI Services

Introduction

Enterprise UDDI Services is a standards-based solution for deploying a private UDDI (Universal Description, Discovery and Integration) service for Standard Edition, Enterprise Edition and Datacenter Edition. UDDI Services can be deployed on an intranet or extranet. UDDI Services is the Web Services infrastructure in Windows .NET Server 2003 that helps companies organize and catalog programmatic resources and provides an efficient mechanism for discovery, sharing and reuse of Web Services. By applying categorization schemes such as Quality of Service, Geography or Organization in UDDI Services, companies can establish a structured and standardized way to describe and discover services. This section provides an overview of the core scenarios, benefits and features of Enterprise UDDI Services in Windows .NET Server 2003.

The most common scenarios for UDDI Services in the enterprise are developer re-use and dynamic configuration.

Core Scenario	Description
Developer Re-Use	When building applications, developers search UDDI for programmatic resources to re-use, such as a tax calculation service. UDDI exposes all of the information needed to invoke a service to make it easy for the developer to include in an application.
Dynamic Configuration	At runtime, an application queries UDDI to discover the current binding information for services and then connects directly to those services. An example of this is a stock broker application that queries UDDI Services first thing in the morning to get configuration information for the different services it consumes such as a stock ticker, customer service applications, settlement services, etc. Using UDDI Services, IT can provide highly available, reliable applications without having to modify client code, using dynamic, flexible infrastructure for Web Services in Windows .NET Server 2003.

Benefits

UDDI Services delivers key strategic benefits to enterprises deploying Web Services. As a core piece of Web Services infrastructure in Windows .NET Server 2003, UDDI Services makes it easy to discover, share and re-use Web Services and other programmable resources, improving developer and IT productivity and resulting in a lower total cost of ownership (TCO) and more reliable and manageable applications.

- Productivity
- Manageable
- Smarter Applications

Benefit	Description
Productivity	Services stores both the technical information to build an application compatible with a web services interface, as well as the information required to successfully bind to that interface at runtime. Enterprise UDDI Services provides developers with a rich mechanism to find each other's services using a rich set of standard or customized classifications, which

	encourages code reuse. With Web Services, enterprise developers can share and re-use code regardless of their development platform. UDDI Services is integrated with Visual Studio .NET and the Office Web Services Toolkit making it easy for developers to locate and re-use Web Services within their application development environment. Easily discover, share and re-use web services when building applications or extending existing enterprise applications. UDDI Services provides developers a central repository of service description and technical binding information, making it easier to re-use existing services and publish new services based on standard and custom categorization schemes. With Web Services, developers can re-use components regardless of their development platform.
Manageable	UDDI Services provides an efficient way to categorize programmable resources on the network. IT administrators can configure applications based on classifications schemes such as quality of service, location or organization during service deployment. For applications that check UDDI for binding information, only an update to UDDI is required to point applications at new services.
Robust, flexible, smarter applications	Using UDDI in applications, you can query UDDI for service and binding information and dynamically adapt at runtime. This results in more robust and smarter applications that consistently deliver a more reliable experience for the end user.

New Features and Improvements

Enterprise UDDI Services enables developers to publish, discover, share, and interact with Web Services directly through their development tools and business applications.

UDDI Services provides support for:

- UDDI API
- Categorization schemes
- Searching, Publication and Coordination
- UDDI Client Support

Feature	Description
UDDI Services	Enterprise UDDI Services is a managed code service in Windows .NET Server 2003. It was developed using the .NET Framework and leverages our experience running the Microsoft public node of the UDDI Business Registry (UBR). UDDI Services is an ASP.NET application that is exposed via a web UI or programmatically via a SOAP interface. UDDI Services automatically publishes its existence and location in UDDI Services so that it is easily discoverable as a Web Service.
Active Directory Integration	UDDI Services leverages many feature of Active Directory. Active Directory provides the authentication and authorization backbone for

	UDDI services. All access and permissions to UDDI services, whether for reading, publishing or coordination are assigned through a set of roles defined during installation within Active Directory. Furthermore, Active Directory provides one of the initial bootstrap mechanisms for finding UDDI Services servers on the network. UDDI Services can optionally be installed as a service within Active Directory and a simple query will return you the list of all UDDI Services on the network that you can query for richer web service information. This feature provides the option to publish the existence and location of a UDDI Services instance in Active Directory if a suitable domain is available.
UDDI API and Web-based User Interface	UDDI Services supports programmatic inquiries via the UDDI API and also includes an intuitive Web interface with searching, publishing, and coordination features that are compatible with Microsoft Internet Explorer 4.0 or later and Netscape Navigator 4.5, or later. UDDI Services supports versions 1.0 and 2.0 of the UDDI Programmer's API, enabling enterprise developers to publish, discover, share, and interact with Web services directly through their development tools and business applications.
Searching & Publication	This feature provides capabilities to query UDDI Services and publish entries via the web-based UI or via the UDDI API.
Coordinator Role	The Coordinator role is an administration feature we added to make management of the data within UDDI Services easier within an enterprise.
Categorization Scheme Management	The Related Category API allows developers to programmatically traverse categorization schemes.
Industry-leading Tools	Microsoft offers UDDI client support through several tools including Visual Studio .NET, the Office XP Web Services Toolkit, and the UDDI SDK. Microsoft Visual Studio® .NET provides native support for UDDI Services through "Add Web Reference," enabling developers to easily discover Web Services and other programmatic resources in UDDI for use in building dynamic applications.
Data Import	This feature allows a UDDI Services Coordinator to import UDDI data from an XML file that complies with a defined schema.
Authentication	UDDI Services supports native UDDI authentication and native Windows authentication via Active Directory.
Roles Administration	IT administrators can easily manage access to UDDI Services functions, such as searching and publishing information, by assigning users to one of four roles that define the level of interaction a user is allowed in UDDI Services: User, Publisher, Coordinator

	and Administrator.
MMC Administration Utility	UDDI Services site administrators can easily configure and remotely administer the UDDI Services server via the Microsoft Management Console (MMC) utility. Site administrators have the ability to backup and restore the UDDI Services database.
Database and Server Configuration	UDDI Services uses MSDE (Microsoft Data Engine) as the default store. We also support Microsoft SQL Server 2000 for high reliability and availability scenarios. UDDI Services may be deployed on a single server or across multiple servers. One option is to distribute the web-based UI and APIs across one or more servers in a typical web farm configuration and run the database on a separate dedicated server with SQL Server™ 2000. Alternately, the web based GUI and APIs can be distributed across one or more servers in a typical web farm configuration and the database installed and run on a clustered instance of SQL Server 2000 using Microsoft's clustering technology. This configuration provides great scalability and reliability.
Activity Monitoring	Administrators have the ability to audit of all authenticated activities performed and the user that performed them.

Summary

Enterprise UDDI Services provides a standards-based solution that provides developers, IT professionals and business decision-makers increased visibility into the enterprise application portfolio while maximizing developer and IT productivity.

Windows Media Services

Introduction

Windows .NET Server 2003 includes the industry's most powerful digital/streaming media server, Windows Media Services. Windows Media Services in Windows .NET Server 2003 is part of the next version of the Windows Media Technologies platform (code named "Corona") that also includes a new Windows Media Player, Windows Media Encoder, Audio/Video Codecs, and Windows Media SDK. For more information on "Corona", see <http://www.microsoft.com/windows/windowsmedia/thirdgen/default.asp>.

Streaming is being embraced by a rapidly growing segment of enterprises. Market Decisions Corp., which routinely measures streaming adoption, found that usage has grown from one-in-ten enterprises in October 1999 to nearly one-in-four, today. Among companies with 5000+ desktops, they found that over 40 percent are using streaming.

Windows Media Services in Standard Edition, Enterprise Edition, and Datacenter Edition is the most reliable, scaleable, and manageable streaming media server ever.

This section provides an overview of scenarios, new features, and benefits of Windows Media Services in Windows .NET Server 2003.

Scenarios

Streaming improves the economics, reliability, and manageability of networks in digital media scenarios. Windows Media Services delivers these benefits to both the enterprise and commercial customers. Enterprise customers want to deliver richer and more immediate communications and training to employees, partners and customers, while at the same time reducing overall expenditures. The goals of commercial customers are to remain competitive and control spending in today's challenging economic climate, while remaining profitable going forward.

Scenario	Description
Corporate Communications	Multicast broadcasting over the corporate intranet enables corporate executives to deliver real-time communications to the entire organization regardless of geographic proximity. For corporations with infrastructure constraints, unicast broadcasts provide a similar reach; however, a multicast broadcast delivers the most economical solution, while conserving network bandwidth. The benefits of a cost-effective and simultaneous alignment of the entire organization to the corporate strategic direction can be realized through a reduction in operating expenses, and improved profits.
Electronic Learning	Corporations that deliver training over the intranet can cost-effectively and efficiently deliver high quality and consistent training to management, employees and channel, regardless of their location or computer device. In this scenario, traditional costs associated with on-location training or videocassette distribution are reduced, and employees always get the most current information. Receiving training when and where they want increases employee productivity.
Commercial Internet Broadcasters	With Windows Media Services, film and music industries can easily and efficiently distribute the highest quality audio and video content to the broadest possible audience. Radio and TV stations can deliver reliable, real-time broadcasts to audiences while at

	the same time leveraging the powerful advertising and logging features to generate and track revenue. Broadcast stations have complete flexibility to customize and dynamically change playlists and insert advertisements or public service announcements at any point during the broadcast without interrupting the audience's viewing experience. All Internet broadcasters will find that Windows Media Services readily integrates into existing environments, and customized distribution solutions can easily be developed to distribute content to edge servers thereby optimizing streaming economics.
--	---

Features and Improvements

Dynamic Content Programming

Windows Media Services provides the capability to automatically program and seamlessly update digital media content on the fly, and broadcast to all devices. Full support for lead-in and interstitial ads ensures a complete TV-like broadcast experience on the internet and improves revenue generation.

Feature	Description
Server-side Playlist	Whether on-demand or live, server-side playlists provide the unprecedented ability to make program changes on-the-fly – change the order of clips, insert a new clip, insert an ad, etc, – during broadcasts and without interruption to the viewer.
Comprehensive Advertising Support	Windows Media Services improves revenue generation through support of a wide variety of advertising types, including lead-ins and interstitial ads, and by easily integrating into 3rd party advertising servers. Advanced usage reporting ensures complete tracking of how and when ads are viewed.
Automatic Playlist Generation	Personalized playlists can be programmed on the server and tailored to individual audience members. Thus, streaming content is more relevant and useful to each user.

Fast Streaming

Combined with the upcoming “Corona” release of the Windows Media Player (see <http://www.microsoft.com/windows/windowsmedia/thirdgen/default.asp> for details), Windows Media Services provides an instant-on, always-on playback experience for users on broadband networks, virtually eliminating annoying buffering delays and interruption when playing digital media content.

Feature	Description
Fast Start	Windows Media Services effectively eliminates buffering time – whether playing a single piece of content, or switching seamlessly between on-demand clips or broadcast channels.
Fast Cache	Fast caching provides an always-on playback experience by streaming content to the Player's cache as fast as the network will allow, reducing the likelihood of an interruption in play due to network issues.
Fast Recovery	Fast recovery virtually eliminates packet corruption and interruption over high latency network connections, for example wireless and satellite, through local packet correction ensuring an uninterrupted viewing experience.

Fast Reconnect	Windows Media Services automatically restores live or on-demand Player/Server and Server/Server connections if disconnected during a broadcast ensuring an uninterrupted viewing experience.
-----------------------	--

Industrial Strength

Windows Media Services supports twice as many simultaneous users with increased reliability and security. Dramatically simplified and more flexible administration reduces management costs.

Feature	Description
More Scalable	Windows Media Services supports twice as many concurrent users at any bandwidth, enabling economical streaming for the largest enterprises and CDNs.
Rich Media Streaming	Windows Media Services extends multicasting of audio and video content, to include HTML content thereby maximizing scalability of rich media content delivery.
Cache/Proxy Platform	Windows Media Services enables developers to easily build streaming cache/proxy solutions and control the customization and extension of native cache and proxy policies. Cache/proxy solutions conserve network bandwidth, decrease network-imposed latency, and decrease the load on Windows Media origin servers.
More Reliable	Plug-ins run in protected memory, ensuring maximum system reliability.
Flexible Administration	Flexible administration through the familiar Microsoft Management Console (MMC), Web Browser, or command-line scripts, enables server management in virtually any environment.
Scenario-based Wizards and Help	New scenario-based Wizards for setup and configuration make it easy to deploy and manage a streaming server. The improved Help system is organized around common audio and video streaming scenarios, which ensures easy deployments.
Secure Content Delivery	Windows Media Services provides secure server-to-server and server-to-client distribution of content using variety of common authentication and authorization mechanisms, including new support for Kerberos and HTTP Digest. Also supports digital rights management for on-the-wire and persistent client-side-security.
Standards Based	Windows Media Services maximizes streaming capabilities and integration by including support for HTTP 1.0/1.1, RTP, RTSP; HTML v3.2; FEC; IPv4/6; IGMPv3; SNMP, WBEM/WMI; SMIL 2.0, SML, XML-DOM; COM/DCOM

Extensible Platform

Windows Media Services empowers application developers and IT professionals to customize digital media solutions via a rich, extensible platform and enables them to create new stand-alone applications:

Feature	Description
Flexible Plug-in Architecture	Enable developers to easily extend the Windows Media Services functionality and integrate with their existing systems and solutions, such as storage systems, billing,

	and logging applications.
Powerful Object Model and Event Mechanism	Enables developers to easily build custom applications for configuring and monitoring Windows Media Services, using standard WBEM/WMI, and the industry's most extensive object model with over 1000 server interfaces.
Broad Programming Language Support	Event plug-ins are supported by familiar programming languages such as C++, C#, VBScript, & Perl.

Summary

The new version of Windows Media Services in Windows .NET Server 2003, combines unparalleled power and security for streaming applications, both in corporate intranets and the internet, through:

Dynamic Content Programming: extending dynamic and flexible programming capabilities enabling on the fly program changes with full advertising support.

Fast Streaming: providing the instant-on, always-on playback experience to audiences using the upcoming "Corona" release of the Windows Media Player.

Industrial Strength: delivering the most scalable, reliable, secure, and manageable media distribution system.

Extensible Platform: integrates and extends easily and completely into existing systems and provides a powerful platform for the development of new solutions.

Feature Comparison Chart

Feature	Improved in Windows .NET Server 2003 New Features in Windows .NET Server 2003	Web	Standard	Enterprise	Datacenter	64- bit
802.1x (wireless network) support	X	X	X	X	X	X
Active Directory	X		X	X	X	X
Active Directory Migration Tool	X		X	X	X	X
All-User Remote Access Service Credential	X	X	X	X	X	X
Application Verifier	X	X	X	X	X	X
Assisted Support - Microsoft Incident Submission and Management	X	X	X	X	X	X
ASP.NET	X	X	X	X	X	X
ATM Support	X	X	X	X	X	X
Auto-Configuration for Multiple Networks Connectivity	X	X	X	X	X	X
Automated System Recovery	X	X	X	X	X	X
Backup Utility	X	X	X	X	X	X
Bandwidth Throttling	X	X	X	X	X	X
Certificate Services	X	X	X	X	X	X
Clustering	X			X	X	X
Command Line Tools	X	X	X	X	X	X
Compatibility Mode	X	X	X	X	X	X
Component Services	X	X	X	X	X	X
Connection Manager	X	X	X	X	X	X
Configuration Check Tool	X				X	X
Credential Management	X	X	X	X	X	X
DHCP with DNS and Active Directory	X		X	X	X	X
Distributed File Service	X	X	X	X	X	X
Disk Management	X	X	X	X	X	X
Disk quota support	X	X	X	X	X	X
Domain Rename	X	X	X	X	X	X
DualView	X	X	X	X	X	X
Encrypting File System	X	X	X	X	X	X
Enterprise UDDI Services	X	X	X	X	X	X
EuroZone Support	X	X	X	X	X	X
FAT32 on DVD-RAM	X	X	X	X	X	X
Fax Service	X		X	X	X	X
File & Print for Mac	X		X	X	X	X
Folder Redirection of My Documents	X	X	X	X	X	X
Forest Trust	X	X	X	X	X	X
Group Policy (part of Active Directory)	X		X	X	X	X
Headless Server	X	X	X	X	X	X

Feature	Improved in Windows .NET Server 2003	New Features in Windows .NET Server 2003	Web	Standard	Enterprise	Datacenter	64-bit
Hot Add Memory		X			X	X	X
I2O support		X		X	X	X	X
Indexing Service	X		X	X	X	X	X
Install Replica from Media; Active Directory		X		X	X	X	X
Intellimirror	X		X	X	X	X	X
Internet Authentication Service	X			X	X	X	X
Internet Connection Firewall		X	X	X	X		
Internet Connection Sharing	X			X	X	X	X
Internet Information Services 6.0	X		X	X	X	X	X
Internet Protocol v6		X	X	X	X	X	X
Internet Protocol security support		X	X	X	X	X	X
Kerberos V5 protocol support	X		X	X	X	X	X
Layer Two Tunneling Protocol support	X		X	X	X	X	X
Lightweight Directory Access Protocol support	X		X	X	X	X	X
Manage Your Server		X	X	X	X	X	X
Managed code development model		X	X	X	X	X	X
Metadirectory Services Support		X		X	X	X	X
Message Queuing		X	X	X	X	X	X
Microsoft Data Engine (MSDE)	X			X	X	X	X
.NET Framework / ASP.NET Framework		X	X	X	X	X	X
Microsoft Management Console	X		X	X	X	X	X
Network address translation	X		X	X	X	X	X
Network Bridge	X			X	X	X	X
Network Load Balancing clusters	X		X	X	X	X	X
Non-Uniform Memory Access (NUMA)		X			X	X	X
Operating system migration, support, and integration		X		X	X	X	X
Password Backup and Restore		X	X	X	X	X	X
Plug and Play	X		X	X	X	X	X
Point-to-Point Protocol over Ethernet Connections		X	X	X	X	X	X
POP3 e-mail service	X		X	X	X	X	X
Print for Unix	X			X	X	X	X
Public key infrastructure and smart card infrastructure		X	X	X	X	X	X
Quality of Service	X		X	X	X	X	X
Recovery Console	X		X	X	X	X	X
Remote Assistance	X		X	X	X	X	
Remote Desktop for Administration	X		X	X	X	X	X
Remote Installation Services	X		X	X	X	X	X

Feature	Improved in Windows .NET Server 2003	New Features in Windows .NET Server 2003	Web	Standard	Enterprise	Datacenter	64- bit
Remote OS Installation		X	X	X	X	X	X
Remote Storage		X		X	X	X	X
Removable & Remote Storage		X	X	X	X	X	X
Resultant Set of Policy (RSOP)		X	X	X	X	X	X
Routing and Remote Access	X		X	X	X	X	X
Safe mode	X		X	X	X	X	X
Server clusters	X				X	X	X
Services for Macintosh	X			X	X	X	X
Session Directory for Terminal Services		X		X	X	X	X
Shadow Copy of Shared Folders		X	X	X	X	X	X
Shadow Copy Restore		X		X	X	X	X
Smart card infrastructure	X		X	X	X	X	X
Software Restriction Policies	X		X	X	X	X	X
Storage Area Network Support (SAN Boot)		X			X	X	X
TAPI 3.1	X		X	X	X	X	X
Terminal Services	X			X	X	X	X
Troubleshooting Diagnostic Tool		X	X	X	X	X	X
User State Migration Tool (USMT)		X	X	X	X	X	X
Virtual private networking	X			X	X	X	X
Voice over IP Support		X	X	X	X	X	
Volume Shadow Copy		X	X	X	X	X	X
VT-UTF8 Support for HyperTerminal		X	X	X	X	X	X
WebDAV Redirector		X	X	X	X	X	X
Web gardens		X	X	X	X	X	X
Windows Management Instrumentation (WMI) Comma	X			X	X	X	X
Windows Media Services	X			X	X	X	
Windows Resource Manager (WRM)		X				X	X
Windows Script Host	X		X	X	X	X	X
Windows Sockets: Direct Path for System Area Networks		X	X	X	X	X	X
Windows Update	X		X	X	X	X	X
Winsock Direct	X		X	X	X	X	X

Windows .NET Server 2003, Windows XP Professional, and Microsoft Office XP: Better Together

Today's businesses need dependable, productive, connected computing across the enterprise. End-users need powerful productivity tools on their desktop. They need access to networked resources like file shares and collaboration tools, and they need fast, reliable communications they can trust. Administrators need a scalable, dependable platform to support back-end services along with management tools that are powerful and easy to use.

Windows .NET Server 2003 on the back end with Microsoft Windows XP Professional and Microsoft Office XP on the front end are natural partners in providing the enterprise with effective computing across the board

Providing Dependable Technologies at a Reasonable Cost

Companies expect technology to create value for their business, and they expect it to do this consistently and efficiently. Dependable computing means robust trustworthy systems and tools that are always fast and always available. For the end-users, this means having confidence that the integrity of your data is protected from malicious or accidental loss. For the Information Technology (IT) professional, it means systems that are secure, reliable and scaleable without being too difficult to manage. The combination of Windows .NET Server 2003 together with Windows XP Professional and Office XP delivers on this demand by combining powerful technologies to protect the security and integrity of your systems with a flexible, scalable server platform.

Windows .NET Server 2003

Active Directory – Active Directory makes it easier to manage your Windows XP Desktop computers by providing a centralized repository for hierarchical information about users and computers on your network. Active Directory incorporates significant improvements in management and performance in Windows .NET Server 2003. The new Metadirectory Management Services (MMS) allows you to unify information from multiple directories in your enterprise.

Group Policy – Group Policy provides centralized configuration and control of your network, enabling you to reduce the costs associated with managing it. Group Policy administration has been greatly simplified in Windows .NET. The Resultant Set of Policy (RSOP) tool gives administrators superior management of policy applied to desktop computers. Software Restriction Policies allow administrators a policy-based way to manage what software gets run in their environment.

Security – Windows .NET Server 2003 brings superior protection against the dangers of malicious and poorly designed code. The Common Language Runtime (CLR) tracks code and checks for errors at runtime that may compromise the security and dependability of your network. Applications written leveraging the .NET Framework make use of common code libraries, reducing the danger that your network will be compromised by poor developer practices.

Storage – Fast and dependable storage is one of the keys to a dependable, productive enterprise. Windows .NET Server 2003 creates flexible, scalable storage for mission critical data using technologies like the Distributed File System (DFS) and improvements in speed and capacity of storage and Storage Area Network (SAN) configurations. Windows .NET Server 2003 also includes

the Microsoft Cluster Service (MSCS) and Network Load Balancing (NLB). Storage is also easier to maintain and manage with an overhauled management interface.

Shadow Copy for Administrators – Shadow Copy Restore gives administrators access to point-in-time backups of network shares. Shadow Copy administration makes it easy for administrators to configure Shadow Copy and find backup copies of resources.

Ease of Deployment and Migration – An operating system that is easy to deploy and migrate means lower costs in time and money. Windows .NET Server 2003 with Windows XP and Office XP clients can make use of a number of powerful deployment tools like Remote Installation Services (RIS) and SysPrep to keep initial costs as low as possible. The User State Migration Tool (USMT) allows administrators to collect and transfer a wide variety of user settings, including software settings, and transfer them to a new desktop as part of a deployment or upgrade.

Microsoft Windows XP Professional with Office XP

Application Recovery – Windows .NET Server 2003 with Windows XP and Office XP clients makes it easier to recover from disasters with features like Document Recovery, AutoRecover and Automated System Restore so that you do not lose critical data in information in case of accident.

Encrypting File System (EFS) – The Encrypting File System is the secure encrypted file system for NTFS volumes. EFS enhances security by providing users with powerful, secure storage. Now with Windows XP Professional and Windows .NET Server 2003, EFS can be used to encrypt offline files and web folders, and EFS volumes can be shared among multiple users.

Shadow Copy for Users – Shadow copy provides point-in-time storage for network shares. Users can easily access backed up versions of files through the Windows explorer by right-clicking on a file or folder.

Enhancing Productivity with Easy to use Tools and Technologies

One of the primary ways in which technology can yield increasing value for the enterprise is by improving productivity globally from the end-user to back-end services. End-users require more powerful productivity tools that integrate seamlessly with back-end systems and other users. IT professionals must be able to configure and manage systems easily and flexibly in order to respond to demand. The end product is not just an enterprise that is more productive, but one that is more responsive to change, able to take advantage of opportunities as they arise. The combination of Windows .NET Server 2003 with Windows XP Professional and Office XP clients achieves these goals by closely integrating back end data and services with the productivity tools that desktop users work with every day.

New Task-Based Design – Both Windows .NET Server 2003 and Windows XP Professional with Office XP have been redesigned for efficiency and ease-of-use. The new task-based design makes it easier to find and carry out common everyday tasks. Users and administrators spend less time hunting around for the answers to problems and more time being productive.

Windows .NET Server 2003

Terminal Services Enhancements – Terminal Services is a Microsoft technology that lets you deliver the full functionality of a virtual Windows Desktop to almost any device. The new Remote Desktop Protocol (RDP) 5.1 brings amazing improvements in Terminal Services performance and functionality.

File and Print Servers – Windows .NET Server 2003 is an excellent platform to provide back-end services like file and print services to Windows XP Professional with Office XP users. Improvements to the Encrypting File System (EFS) and the Distributed File System (DFS) allow Windows .NET Server 2003 to provide storage that is faster and more reliable than ever before. Print services have also been improved, including support for print clusters.

Microsoft Windows XP Professional with Office XP

Smart Tags – Smart Tags are context-sensitive menus which can be embedded in Office XP documents and web pages, allowing users to connect to information and services relevant to the job they're doing. Smart Tags are a great way to connect users of the Microsoft client platform of Windows XP Professional and Office XP with back-end databases, line-of-business applications, productivity tools and information stores.

Connecting Users, Customers and Partners Together

As bandwidth become more available and computer become cheaper and more powerful, demand for powerful and fast communications has grown. Companies need software that's ready to function in a global connected environment. They need to take advantage of opportunities for better communications within their company and beyond to their partners and customers. Windows .NET Server 2003 with Windows XP Professional and Office delivers this by providing you with a platform that's powerful and scalable enough to act as the platform for a host of connected technologies as well as tools that allow end users to communicate more effectively.

Multilanguage Computing – Worldwide computing presents serious challenges to the global enterprise. The Multilingual User Interface (MUI) for Windows .NET Server 2003, Windows XP Professional and Office XP Professional allows you to switch the interface of your operating system and applications, providing you with multilingual computing capabilities. The MUI is binary independent, so you can deploy one version of software worldwide, resulting in considerable savings in deployment and support costs.

Windows .NET Server 2003

Internet Authentication Service (IAS) – Windows .NET Server 2003 provides centralized management of dial-up Virtual Private Network (VPN) users through the Internet Authentication Service (IAS). IAS in Windows .NET Server 2003 allows you to provide quality support for Windows XP Professional with Office XP users to dial-up and access networked resources.

Internet Information Services (IIS) 6.0 – Windows .NET Server 2003 includes the latest release of Windows Server's web services, Internet Information Services (IIS) 6.0. With IIS, you can serve and host web pages, applications and web services on a dependable, scalable platform, allowing your enterprise to make the best possible use of the web.

Web Services – Web Services are building-block applications that can be aggregated into full business solutions. Windows .NET Server 2003 is the platform of choice to create, distribute and host XML-based web services, enabling you to quickly develop web-based solutions and productivity tools as opportunities are identified.

Multimedia Services – Microsoft has completely redesigned the multimedia services in Windows .NET Server 2003 in order to provide high quality multimedia across your network. Multimedia services

are now faster and more robust and include new capabilities for dynamic arrangement of content allowing you to meet today's multimedia demands.

Microsoft Windows XP Professional with Office XP

MSN® Messenger – MSN Messenger allows users to communicate more effectively by giving them real-time messaging, document sharing and online conferencing. The Windows XP Professional with Office XP desktop includes full integration with MSN Messenger.

Remote Assistance – Support costs are a significant part of the total cost of owning software. Effective and efficient support helps ensure end-use productivity while keeping costs down. Remote Assistance is a new feature in Windows XP Professional that allows support staff to interact with users and take over remote control of their desktops with their permission in order to carry out support tasks more easily.

Virtual Private Networking (VPN) – Giving mobile users access to network resources and services has always been a challenge. With Virtual Private Networking (VPN) on Windows XP Professional supported by Windows .NET Server 2003, mobile users can dial-up to your network securely and easily.

Summary

Windows XP Professional with Office XP is Microsoft's most advanced desktop for end users. Microsoft Windows .NET Server 2003 is the latest server operating system from Microsoft. Together, they provide an unprecedented level of dependability, productivity and connectivity to the enterprise. The superior management capabilities of Windows .NET Server 2003 create value for enterprise customers by allowing control and management of resources quickly and easily. The end result is a full computing solution that meets the needs of businesses while keeping costs down.

Related Links

For further information about the Windows .NET Server 2003 Family, see the [Windows .NET Server 2003 Web site](http://www.microsoft.com/windows.netserver) at <http://www.microsoft.com/windows.netserver>. Among the many resources on the site are in-depth technical articles describing many of the new and improved technologies and features in Windows .NET Server 2003. Link directly to the Technical Overviews page at <http://www.microsoft.com/windows.netserver/techinfo/overviews/default.mspx>.

Supporting information also can be found for:

- Microsoft .NET at <http://www.microsoft.com/net>
- Windows Server Operating Systems at <http://www.microsoft.com/windows/WinHistoryServer.asp>
- Windows XP Professional Operating System at <http://www.microsoft.com/windowsxp/pro/default.asp>
- Windows 2000 Operating Systems at <http://www.microsoft.com/windows2000/default.asp>
- Microsoft .NET Enterprise Servers at <http://www.microsoft.com/servers/default.asp>
- MSDN at <http://www.microsoft.com/msdn>
- TechNet at www.microsoft.com/technet