



Why Upgrade From Windows NT 4.0 to Windows Server 2003

Microsoft Corporation

Published: November 2002

Abstract

Microsoft® Windows® Server 2003 provides many new tools, services, and features that make a compelling case for upgrading from Windows NT® Server 4.0. This white paper explains the immediate benefits of upgrading without installing the Active Directory® service and then addresses the significant management and cost-saving benefits provided by Active Directory. The rest of the paper examines enhancements in key server roles including, file and print, secure wired and wireless connectivity, Active Directory identity management, management services, and secure and reliable Web servers (Internet Information Services 6.0). The paper concludes by showing how Windows Server 2003 enables server consolidation.

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

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

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

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2003. Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, FrontPage, Visual Basic, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Contents

Introduction	1
Benefits of Upgrading to Windows Server 2003	2
Benefits of Upgrading to Windows Server 2003 Without Active Directory	2
Improved Reliability	2
Improved Availability	2
Increased Scalability	3
Immediate Advantages of Upgrading to Windows Server 2003	3
Benefits of Upgrading to Windows Server 2003 With Active Directory	3
The Need for Active Directory	4
Finding Information Quickly.....	4
Easier to Upgrade to Active Directory	4
Improved Management with Group Policy	5
Migrating By Server Role	6
File and Print Productivity	7
File and Print Service Improvements	7
Storage Improvements	8
Secure Wired and Wireless Connectivity	9
Windows Server 2003 is More Secure Than Windows NT 4.0	9
Features Enabling Secure Wired and Wireless Connectivity.....	9
Firewall Security	10
Managing Network Security	11
Easier-to-Use Active Directory	12
Active Directory in Windows Server 2003	12
Active Directory Identity Management	12
UDDI.....	14
Easier-to-Use Management Services	15
Deploying Secure and Reliable Web Servers	17
IIS 6.0—A New Request Processing Architecture	17
New Performance and Scalability Features.....	17

Preliminary Testing Shows Significant Performance Increases.....	19
Securing IIS.....	19
Managing IIS.....	21
Server Consolidation	23
Improving Availability.....	23
Enabling Interoperability.....	24
Boosting Performance.....	24
Consolidating Application Servers: Side-By-Side Application Support.....	24
Windows System Resource Manager	24
Related Links	26

Introduction

Organizations today are requiring more and more IT services and features to meet the ongoing business demands they face. Therefore server operating systems must support an extensible array of services that provide for availability, reliability, scalability, and more—all within a secure environment. Microsoft Windows® Server 2003 provides many new tools, services, and features that make a compelling case for upgrading from Windows NT® Server 4.0.

You can realize immediate benefits by simply upgrading a server to Windows Server 2003. You can also realize many additional benefits by deploying the Active Directory® service. The following table highlights these benefits.

Overall Server Role	Upgrade a Server to Windows Server 2003	Upgrade a Domain to Active Directory
IT Infrastructure	<ul style="list-style-type: none"> ▪ Robust security including enhanced PKI and Kerberos. ▪ Unified management ▪ Secure remote and wireless access 	<ul style="list-style-type: none"> ▪ Centralized administration ▪ Easier-to-use Group Policy management ▪ Certificate auto enrollment
Application Platform	<ul style="list-style-type: none"> ▪ XML Web services via Microsoft .NET–connected technologies ▪ IIS 6 with at least double the performance of IIS 4. ▪ Flexible application security 	<ul style="list-style-type: none"> ▪ Directory-enabled applications ▪ Single sign-on ▪ Microsoft Passport, role-based access control
Information Worker Infrastructure	<ul style="list-style-type: none"> ▪ Shadow copy Restore ▪ Encrypted file system ▪ Offline files and folders 	<ul style="list-style-type: none"> ▪ Roaming profiles ▪ Documents “follow” you ▪ Simple printer access

This white paper explains these benefits further and addresses key server roles for some of the major areas in which Windows Server 2003 can help organizations become more productive.

Benefits of Upgrading to Windows Server 2003

Windows Server 2003 takes the best of Windows 2000 Server technology and makes it easier to deploy, manage, and use.

Benefits of Upgrading to Windows Server 2003 Without Active Directory

Organizations upgrading to Windows Server 2003 can realize immediate benefits—even without deploying Active Directory. The result: Improved reliability, availability, and scalability.

Improved Reliability

The following features improve uptime and stability while helping system administrators maintain a healthy and reliable server environment:

- **Device Driver Resiliency: Block Defective Drivers.** This feature programmatically keeps users from installing and loading drivers that are known to crash or hang the operating system. If a driver is installed and the driver is in the driver blocking database, the user will be notified that the driver will not be installed. This protects the user from inadvertently installing or loading a device driver that may impact the server.
- **Device Driver Roll Back.** This lets you replace a device driver with the previously installed version. If you install a new device driver that causes system instability on the server, you can restore or roll back to the previous device driver.
- **Device Drivers: Last Known Good Files.** When you update a driver, the operating system saves a copy of the driver that was used the last time the computer was started. If the new driver does not work properly and prevents the server from starting, you can boot the server into Safe Mode and use the “last known good configuration.” This restores the driver to the previous version and allows the server to regain operation.
- **System File Protection.** System file protection serves the goal of maintaining a stable and reliable operating system by preventing replacement of certain monitored system files except by trusted sources, such as service pack installations or Windows Update. System File Protection helps maintain a healthy core system, protecting core system files from corruption, deletion, and modification.
- **Application Compatibility.** The Limited User Access (LUA) Compatibility feature provides support for running older applications under a limited or restricted user account. Because applications written for the Windows 95, Windows 98, and Windows Millennium architecture did not have to address registry or file system security, these applications could write their state information and update data files in folders that are restricted to administrators. Windows Server 2003 resolves this issue and enables users to continue using their older applications.

Additional reliability features are explained in the section below, [Migrating by Server Role](#).

Improved Availability

Windows Server 2003 provides greatly improved availability compared with Windows NT Server 4.0. For the greatest availability, organizations should consider Windows Server 2003, Enterprise Edition, and Windows Server 2003 Datacenter Edition. The following features provide enhanced availability:

- **Cluster Service (MSCS).** 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.
- **Network Load Balancing (NLB).** Available in all editions of the Windows Server family, this service load balances incoming Internet Protocol (IP) traffic across clusters. 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.

Additional availability features are explained in [Migrating by Server Role](#).

Increased Scalability

Windows Server 2003 includes the following features that enable greater scalability:

- **64-bit Processor Support.** 64-bit versions of Enterprise Edition and Datacenter Edition can take advantage of the latest 64-bit hardware for increased scale-up and scale-out capabilities. This increases scalability and reliability for memory-intensive applications such as mechanical design, computer-aided design (CAD), professional graphics, high-end database systems, scientific applications, data warehousing, business intelligence, and Web hosting.
- **NUMA Support.** The Non-Uniform Memory Access (NUMA) in multi-processor systems provides greater performance and scalability. Existing servers can do more work, or the same work can be done by fewer servers, leading to lower costs.
- **Increased Memory Support.** There is support for up to 512 GB memory on 64-bit systems and 64 GB memory on 32-bit systems.
- **Greater SMP Support.** Windows Server provides 4-way, 8-way, and 32-way symmetric multiprocessing (SMP).

Additional features that enhance scalability are included in [Migrating by Server Role](#).

Immediate Advantages of Upgrading to Windows Server 2003

Organizations still using Windows NT Server 4.0 have much to gain by migrating to Windows Server 2003—even without deploying Active Directory. They have even more to gain by realizing the efficiency and productivity advantages provided by Active Directory.

Benefits of Upgrading to Windows Server 2003 With Active Directory

Windows Server 2003 includes many enhancements to Active Directory. It includes several utilities to upgrade installations from Windows NT 4.0 or Windows 2000. Furthermore, Windows Server 2003 enhances the administrator's ability to efficiently configure and manage Active Directory even in very large enterprises with multiple forests, domains, and sites.

The Need for Active Directory

If you look closely at the computer systems in many organizations today, you will likely find numerous different directories for functions such as e-mail, human resources, security, voice mail, payroll, and more. You name it and there is a directory for it—each an island of special records and database entries that must be updated separately from everything else and, in many cases, duplicated manually across the network. The larger the organization, the greater the potential variety of directories and the effort required to keep them updated.

So, not surprisingly, organizations have long been seeking a solution to control the costs of managing their computer-based directories. Meanwhile, deploying and leveraging a single, unifying directory service has become increasingly critical in the Internet economy where businesses are retooling and rethinking how they are going to compete.

Active Directory goes a long way toward delivering this infrastructure while helping reduce the costs of maintaining a workstation or PC.

With Active Directory, employees can quickly find information about all the resources connected to your network. Administrators can manage the network from a central location—whether the enterprise spans cities, countries, or hemispheres.

Ultimately, the efficiencies introduced in Active Directory can reduce IT costs and help your organization get more work done.

Finding Information Quickly

At the simplest level, Active Directory is a database of information about users, computers, printers, and just about any computer-related item in the enterprise. Users benefit from Active Directory by being able to quickly find what they need—anywhere in the network. For example, Active Directory can serve much like a Yellow Pages by automatically locating the nearest printer, freeing users from having to know the correct name or address path of the printer.

Easier to Upgrade to Active Directory

Improved migration and management tools along with the ability to rename Active Directory domains make deploying Active Directory significantly easier than when the directory service was first introduced in Windows 2000 Server.

Migration and planning are more efficient with the following:

- **ADMT 2.0.** 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 2.0 now allows migrating passwords from Windows NT 4 to Windows 2000 and Windows Server 2003 or from Windows 2000 to Windows Server 2003 domains.
- **Domain Rename.** This supports changing the Domain Name System (DNS) and/or NetBIOS names of existing domains in a forest, keeping the resulting forest still “well formed.” Administrators have greater flexibility in changing the Active Directory structure after it is deployed. Design decisions are now reversible, which benefits organizations that may be involved in a merger or significant restructuring.
- **Schema Redefine.** The flexibility of Active Directory has been enhanced to allow the deactivation of attributes and class definitions in the Active Directory schema. Attributes and classes can be redefined if an error was made in the original definition.

Improved Management with Group Policy

Organizations still using Windows NT 4.0 can significantly lower costs by taking advantage of the efficiencies enabled by Group Policy and Active Directory. Although Windows NT 4 provided rudimentary tools to set policies, it was done on a server-by-server basis and was hard to administer. Group Policy in Windows Server allows for the simple setting of policies for desktop and servers that automatically can be applied to as many desktops and servers as necessary via Active Directory, as shown in Figure 1 below.

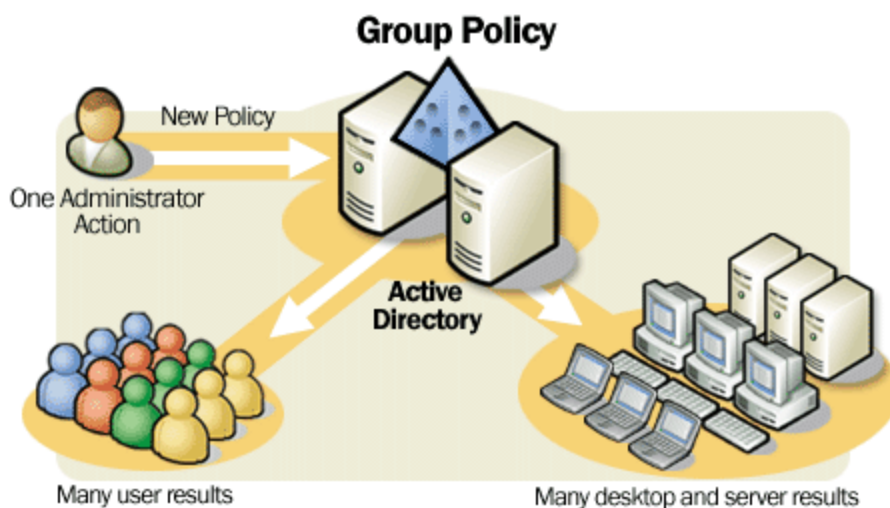


Figure 1. Managing users and computers with Group Policy

Group Policy in Windows Server 2003 provides benefits in the following areas:

- **Enhanced Security.** Administrators can easily define and automatically enforce software security policies.
- **Improved Customer Satisfaction and Reduced Help Desk Costs.** Administrators can enforce standardized desktop and server environments. This capability decreases the risk of broken software configurations and user error, while improving the IT organization's ability to troubleshoot problems.
- **Increased Data Safety and Availability.** Administrators can provide automated folder redirection, data backup and data recovery via Group Policy.
- **Flexible Control Over the Computing Environment.** Administrators can define and enforce organizational standards through Group Policy, and can rapidly re-configure Group Policy settings to adapt to changing business requirements. Group Policy implementations scale easily—from small work group environments all the way up to high-end data centers—and simulate and validate the impact of any changes before applying them to production environments.
- **Increased Productivity.** Administrators can manage an entire group of users and IT assets as easily as managing a single entity. Group Policy lets administrators respond rapidly to required changes in group configurations or policy enforcements, a benefit that helps organizations run their IT operations more effectively. Plus scripting of Group Policy operations can provide even greater IT workload efficiencies.

Migrating By Server Role

Designed to help organizations improve their efficiency and productivity, Windows Server 2003 provides many incentives to migrate from Windows NT Server 4.0. Top scenarios for Windows NT 4.0 customers include the following:

- File and print productivity.
- Secure wired and wireless connectivity.
- Easier-to-use Active Directory.
- Easier-to-use management services.
- Secure and reliable Web servers (Internet Information Services 6.0).

File and Print Productivity

As more business information becomes available in digital form, it can be analyzed creatively, searched faster, updated more easily, and shared more broadly. The substantially increased volume of information being stored by most organizations—particularly large files such as digital images—also presents significant new management challenges. Windows Server 2003 addresses these expanding requirements with support for sophisticated file, print, and storage services that:

- Maintain data availability and security.
- Ease deployment and management.
- Integrate well with existing infrastructure.

File and Print Service Improvements

Enhanced file and print services can deliver significant cost savings, resulting in improved performance, higher availability, better manageability, and stronger security:

- **NTFS Journaling File System.** This supports file system recovery, extremely large storage media, and long file names.
- **Dynamic Volume Management.** Administrators can perform many tasks while the server is online, without impacting users, such as add new volumes, extend existing volumes, remove or add a mirror volume, or repair a RAID 5 array.
- **Distributed File System (DFS) Improvements.** 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. DFS is enhanced for Windows Server 2003, Enterprise Edition, and Windows Server 2003, Datacenter Edition, by allowing multiple DFS roots on a single server. You can use this feature to host multiple DFS roots on a single server, reducing administrative and hardware costs of managing multiple namespaces and multiple replicated namespaces. Using the Active Directory service, DFS shares can be published as volume objects and administration can be delegated. Other 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.
- **Hot Add Memory.** This allows ranges of memory to be added to a computer and be made available to the operating system and applications as part of the normal memory pool without rebooting the computer or forcing downtime.
- **Automated System Recovery (ASR).** This improves productivity by enabling a one-step restore of operating system, system state, and hardware configuration in disaster recovery situations. This makes rebuilding a server much easier and faster because no actual software has to be reloaded.
- **Clustered Print Services.** Clustered print services can reliably serve hundreds, or even thousands, of printers from a single two-node print server cluster.

Storage Improvements

In today's IT environment, the explosion of corporate data is forcing companies to deploy ever larger and more advanced storage systems. The Windows Server 2003 family introduces 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 SANs. Volume Shadow Copy services and Volume Disk Services (VDS) are the latest additions to the improved storage services architecture in Windows Server 2003. The Volume Copy service and VDS provide heterogeneous interoperation of storage hardware, storage software, and applications. Specifically, storage features include:

- **Volume Shadow Copy service.** Known in the industry as "snapshots," the Volume Shadow Copy service provides an infrastructure for creating a point-in-time copy of a single volume or multiple volumes. The Volume Shadow Copy service is used for managing data from direct attached storage to storage area networks (SANs). Volume Shadow Copy service coordinates between line-of-business applications, backup applications, and storage hardware to enable application-aware data management. Volume Shadow Copy service-aware solutions can produce much-higher-quality shadow copies than other technologies because of its ability to integrate with business applications and to coordinate with the storage hardware. As a result, high-fidelity backup recovery and data mining are possible without significantly affecting performance.
- **Volume Disk Services (VDS).** The Virtual Disk Service enables multi-vendor storage devices to interoperate in Windows. VDS has application programming interfaces (APIs) to storage hardware and to management programs that manage the storage hardware. Administrators can discover multi-vendor storage devices and configure those resources via a unified interface. Without VDS, typically each vendor's storage device had its own management interface.
- **Shadow Copy Restore.** Once 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.
- **Multipath I/O (MPIO).** Multipathing is a high availability function that provides multiple paths from the host to the external storage device. Although MPIO is not a feature of the operating system, the MPIO Driver Development Kit (DDK) allows storage vendors to create interoperable multipathing solutions. Up to 32 paths are supported. Load balancing is an additional benefit that improves performance.
- **Storage Area Network (SAN) Support.** Storage Area Networks are significantly easier to use in Windows Server 2003. Administrators can control the mounting of volumes with the aid of a SAN friendly button, a benefit that protects volumes from unintentional access. Improved handling of fiber channel SANs and improved SAN Host Bus Adapter (HBA) interoperability further eases administration. With vendor support, the ability to boot from SAN is greatly enhanced in Windows Server.
- **Open File Backup.** The backup utility included with Windows 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 open files accessed by users are also backed up.

Secure Wired and Wireless Connectivity

Windows Server 2003 is More Secure Than Windows NT 4.0

Efficient and secure networked computing is more important than ever for a business to remain competitive. Windows Server 2003 contains important remote access and wireless LAN features and functions that are not available in Windows NT 4.0. Windows Server 2003 enables your organization to take advantage of secure mobile access within a secure infrastructure.

Today, organizations must strike a balance between enhanced workforce productivity enabled by mobile access capabilities and the increased expense of providing dial-up connections, leased phone lines, and secure wireless. Taking advantage of the remote access and WLAN services available in Windows Server 2003—which use the same infrastructure for wired and wireless network access—avoids added infrastructure costs.

When you migrate to Windows Server 2003 your organization will have access to a secure built-in public key infrastructure that supports certificate-based authentication for wired and wireless networks, along with autoenrollment and autorenewal features that make it easy to deploy smart cards and certificates across the enterprise.

Using the strong authentication and encryption technologies that are a part of virtual private networks (VPNs) in Windows Server 2003, your organization can use the Internet as a corporate wide area network (WAN) and provide employees with secure local telephone, digital subscriber line (DSL), cable modem access, or other broadband connections, as shown in Figure 2 below.

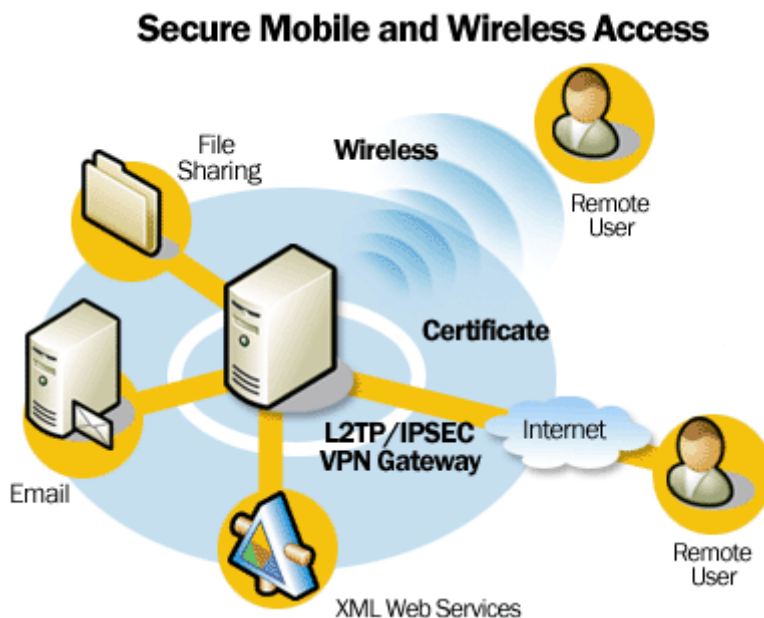


Figure 2. Enabling remote access with VPN and wireless networking

Features Enabling Secure Wired and Wireless Connectivity

Upgrading to Windows Server 2003 is a good choice if your company plans to provide wireless access to the corporate network because wireless support is not possible using Windows NT 4.0.

Windows Server 2003 provides a secure connection to the corporate network and its resources by supporting standardized 802.1X protocols, an integrated public key infrastructure (PKI), password or certificate-based

access, and integrated extensible authentication protocol (EAP) security. Enhancements that enable secure wired and wireless connectivity include the following:

- **Single Sign-On.** Single sign-on to Windows-based network resources improves password secrecy and simplifies password management and lowers help desk requests.
- **Kerberos Authentication.** Full support for Kerberos version 5 protocol provides fast, single sign-on to Windows resources, as well as other environments that support this protocol.
- **Internet Authentication Services (IAS).** Using IAS, the Windows Server Family makes it easier to deploy high-scale solutions for authenticated network access control in wired, wireless, and remote access scenarios.
- **Smart Cards.** Automatic smart card enrollment and self-registration authority features provide enhanced security for enterprise users by adding another layer of authentication.
- **Certificate Services.** Certificate Services is the component in the Windows Server family that is used to create and manage certification authorities (CAs). A CA is responsible for establishing and vouching for the identity of certificate holders. This provides an easy way to create and manage a certificate server.
- **Certificate Autoenrollment and Autorenewal.** 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. This lowers the time and energy it takes to manage a PKI infrastructure and reduces the risk of data loss through unauthorized access.
- **Easier PKI Deployment.** Improvements in PKI dramatically reduce the amount of resources needed to manage X.509 certificates and lower the time necessary to certificate enable the infrastructure. Windows Server makes it possible to automatically enroll and deploy certificates to users. As certificates expire, they can be automatically renewed.
- **Protected EAP (PEAP).** Using the Protected Extensible Authentication Protocol (PEAP), organizations have the option of using Windows domain passwords for authenticated and encrypted wireless communication without having to deploy a certificate infrastructure. This allows flexible authentication without the necessity of rolling out a Public Key Infrastructure (PKI) deployment.

Firewall Security

Internet Security and Acceleration (ISA) Server 2000 provides an extensible enterprise firewall and Web cache server that integrates with Windows Server 2003 for policy-based security, acceleration, and management of internetworking. ISA Firewall services provide enterprise-level security for your network connection. This firewall is straightforward to manage; provides substantial network protection; detects and reacts upon an intrusion; and facilitates operational requirements, such as VPN tunneling and bandwidth rules.

ISA Server builds on Windows Server 2003 security, directory services, VPN, and bandwidth control. Whether deployed as separate cache and firewall servers, or in integrated mode, ISA Server improves Internet access speed, maximizes employee productivity, and enforces network security policies and Internet usage policies for organizations of all sizes. ISA Server is a highly effective tool for implementing your organization's overall security policy.

Managing Network Security

An aspect critical to network security is the ability to effectively and efficiently manage the tools and resources that implement your organization's security policy. ISA Server is closely integrated with Windows Server 2003 and provides robust management and dependable security. The management interface assures that your network security policy is configured correctly, and using familiar scripting interfaces via Windows Scripting Host, you can automate the configuration of ISA Server parameters to match your security policies.

Easier-to-Use Active Directory

Active Directory in Windows Server 2003

Active Directory in Windows Server 2003 lets your organization take advantage of existing IT investments, and extend those advantages to your partners, customers, and suppliers by deploying key features like cross-forest trusts, as well as Microsoft .NET Passport integration.

Windows Server 2003 makes it much easier to use Active Directory and includes new features, such as cross-forest trusts, the ability to rename domains, and the ability to deactivate attributes and classes in the schema so that their definitions can be changed.

Active Directory Identity Management

In most Windows NT 4 or other enterprise environments, many individual applications or systems have their own user database or directory to track who is permitted to use that resource. Each one of these acts as an island of special records and database entries that must be updated separately from everything else and, in many cases, duplicated manually across the network. Inefficiencies stemming from this approach to identity management can have significantly unfavorable financial, productivity, security, and customer service consequences for the enterprise.

Active Directory in Windows 2000 gave users access to different parts of the network with a single sign-on. This greatly reduced the number of passwords users have to remember and enter, and made moving from one application or file share to another much simpler. At the same time, Active Directory in Windows 2000 supported a strong security model that helps prevent unauthorized users from accessing your private corporate information.

Organizations can realize significant advantages from consolidating identity data around strategic directory services. This is because the number of directories where administrators must store and maintain identity data actually decreases.

Active Directory provides the unique role of managing Windows Server 2003 identities alongside the many identities that are scattered in other systems and platforms, in addition to its ability to control security policy and access to other resources. As a result, Active Directory can be relied on as the authoritative store for identity, authentication and authorization information which can be extended to other applications, systems and platforms. Features enabling improved Active Directory identity management include:

- **Cross-Forest Trust.** 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. This provides the flexibility to account for the need for some divisions or areas to have their own forest, yet maintain benefits of Active Directory.
- **Active Directory Application Mode (AD/AM).** Active Directory in Application Mode (AD/AM) is a new mode of Active Directory that addresses certain deployment scenarios related to directory-enabled applications. AD/AM runs as a non-operating system service and, as such, does not require deployment on a domain controller. Running as a non-operating system service means that multiple instances of AD/AM can run concurrently on a single server, with each instance being independently configurable. This provides important e-commerce benefits, allowing Active Directory to be used for eBusiness/external facing usage and using Active Directory expertise for eCommerce directory saves

money; lower training costs. **Note:** AD/AM will be released as a separate component with Windows Server 2003.

Large organizations in particular can benefit from enhanced trusts that can enable greater efficiencies for sharing and management of information across organizational divisions, as shown in Figure 3 below.

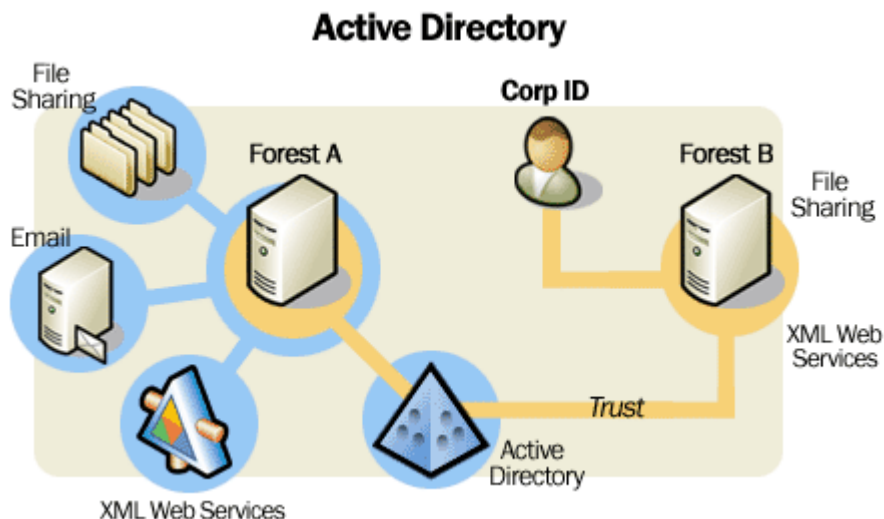


Figure 3. Improved cross forest trust enhances identity management

- Microsoft Metadirectory Services (MMS).** The capability to integrate identity information across multiple repositories, systems and platforms is provided by Microsoft Metadirectory Services 2003 (MMS), which augments Active Directory by providing broad interoperability capabilities. MMS allows a company to integrate Active Directory with a wide variety of identity repositories such as SUNOne/iPlanet directory, Lotus, Novell and Oracle. MMS provides a number of benefits including:
 - Administrative Cost Reduction.** MMS ensures consistency and data integrity throughout your enterprise by automatically propagating and brokering the changes that occur in your disparate systems. Powerful brokering capabilities allow you to take control of how and when these changes are maintained and processed. By translating and interchanging identity information across heterogeneous systems you can now provide consistent and accurate representation of identity information across heterogeneous systems.
 - Business Process Integration.** MMS includes powerful provisioning capabilities that allow you to automatically provision NOS, e-mail, other accounts or services across your enterprise. Directory-enabled account provisioning allows you to reach new levels of efficiency by reducing the amount of manual processing that must occur between systems—when you, for example, hire a new employee.
 - Improved Consistency and Data Integrity.** MMS allows you to enforce ownership of identity information across the enterprise. Without the ability to assign and enforce ownership, identity data can lose integrity. For example, without ownership of an employee's "title" being defined in the human resources system users might have the ability to their own title from the e-mail system's address book. With multiple identity repositories, identity ownership becomes increasingly

important. MMS can ensure that data that has been improperly changed is changed back to the proper value based on which system "owns" that particular attribute.

- **Increased Security.** MMS ensures that the information throughout the enterprise is consistent and up-to-date. Coupled with the integration of business rules and provisioning any changes in an employee's status can be propagated throughout your enterprise quickly and efficiently. For example, when an employee leaves the organization MMS can automatically suspend their accounts thereby reducing the risk of a security breach.

UDDI

Windows Server 2003 includes Enterprise UDDI Services, a dynamic and flexible directory infrastructure for XML Web services. This standards-based solution enables companies to run their own UDDI (Universal Description, Discovery and Integration) directory for intranet or extranet use, making it easy to discover Web services and other programmatic resources. Developers can easily and quickly find and re-use the Web services available within the organization. IT administrators can catalog and manage the programmable resources in their network. Enterprise UDDI Services also helps companies build and deploy smarter, more reliable applications.

Easier-to-Use Management Services

In a Windows NT Server 4.0 environment, administrators were limited to system policies and the ability to specify basic desktop configurations and some security settings. Managing large groups of users and computers was difficult and costly.

Windows Server 2003 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 Server provides centralized, customizable management services to reduce total cost of ownership (TCO).

Change and configuration management features first introduced with Active Directory in Windows 2000 have been improved. Group Policy, in particular, includes several key improvements that will make it easier to use and manage. The following features provide enhanced management in Windows Server 2003:

- **Group Policy Management.** In conjunction with Windows Server 2003, Microsoft is releasing a new Group Policy management solution that unifies management of Group Policy. The Microsoft Group Policy Management Console (GPMC) provides a single solution for managing all Group Policy–related tasks. 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. Highlights include new functionality such as backup, restore, import, copy, and reporting of Group Policy objects (GPOs). These operations are fully scriptable, which lets administrators customize and automate management. Together these advantages make Group Policy much easier to use and help you manage your enterprise more cost-effectively.
- **Managing Security.** Windows Server 2003 was designed to make it easier to both manage security and protect the network from outside threats. Software restriction policies protect your computing environment from untrusted software by allowing you to specify the software that is permitted to run. And when updates are released, a new infrastructure is available for administrators to acquire and centrally manage software updates. Because many corporations do not want their systems or users going to an external source for updates without first testing these updates, Microsoft is providing a version of Windows Update for installation inside your corporate firewall, as explained below.
- **Microsoft Software Update Services (SUS).** This allows customers to install a service on an internal Windows 2000 or Windows Server-based server that can download all critical updates as they are posted to Windows Update. Administrators can also receive e-mail notification when new critical updates have been posted. SUS allows administrators to very quickly and easily deploy the most critical updates to their servers as well as desktop computers running Windows 2000 Professional or Windows XP Professional. SUS is currently available as an add-on to Windows 2000 Server. For more information, see the [SUS Web site](#).
- **Command-line Support.** Windows Server 2003 provides a significantly enhanced command-line infrastructure, allowing you to perform most management tasks without using a graphical user interface. Of special importance is the ability to perform a wide range of tasks by accessing the information store enabled by Windows Management Instrumentation (WMI). This WMI command-line (WMIC) feature provides a simple command-line interface that interoperates with existing shells and utility commands and can be easily extended by scripts or other administration-oriented applications. Overall, the greater

command-line functionality in the Windows Server family combined with ready-to-use scripts rivals the power of other operating systems often associated with higher cost of ownership. Administrators accustomed to using the command line to manage UNIX or Linux systems can continue managing from the command line in the Windows Server family.

- **Remote Desktop for Administration.** Remote Desktop for Administration builds on the remote administration mode of Windows 2000 Terminal Services. In addition to the two virtual sessions that are available in Windows 2000 Terminal Services remote administration mode, an administrator can also remotely connect to the real console of a server
- **Powerful Deployment Tools and Services.** Improvements in Windows Server 2003 make it easier to manage deployment and migration. Remote Installation Services (RIS) has been extended to give you greater flexibility and precision in deploying specific configurations across the network. User state migration is more powerful, giving you the ability to efficiently migrate files and settings for large numbers of users. Windows Installer eases the process of customizing installations, updating and upgrading applications, and resolving configuration problems.

Deploying Secure and Reliable Web Servers

Internet Information Services 6.0 (IIS 6.0) and Windows Server 2003 introduce many new features for Web application server management, performance and scalability, availability and reliability, and security.

IIS 6.0—A New Request Processing Architecture

Web site and application code is increasingly complex. Custom applications and Web sites hosted in customer environments might contain some imperfect code. Therefore, the Web application hosting infrastructure needs to be an active manager of the runtime environment by automatically detecting memory leaks, access violations, and other errors. When these conditions occur, the underlying architecture needs to be fault tolerant, actively recycle or restart processes as necessary, and continue to queue requests—without interrupting the user experience. Specifically, architectural improvements that enable IIS 6.0 to reliably host Web applications include the following:

- **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, as well as providing a consistent, "always available" view of the Web application to the client by queuing requests in the kernel for the Web application worker processes. HTTP.sys is also responsible for overall connection management, bandwidth throttling, and Web server logging.
- **Application Pools.** Application pools define a set of Web applications that share one or more worker processes. Each application pool is separated from other application pools by process boundaries. In addition, application pools pull requests directly from the kernel-mode HTTP.sys driver instead of directing them through a single user-mode process where other applications can also run. This results in better uptime and lower maintenance for Web servers.
- **Rapid Fail Protection.** When a worker process fails, the WWW service detects the failure and takes action, which typically includes logging the event and restarting the worker process. If this happens repeatedly, IIS can be configured to not restart the worker process to prevent repeated crashing, which could affect the rest of the operating system by taking resources to always restart the worker process.
- **Worker Process Recycling.** Today, many businesses and organizations have problems with Web applications that leak memory, suffer from poor coding, or have indeterminate problems, which appear over a period of time. This forces administrators to reboot or restart their Web servers periodically. In previous versions of IIS, it was not possible to restart a Web site without an interruption of the entire Web server. Worker Process Recycling allows customers to configure the WWW service to recycle the worker processes serving their application pools periodically based on a number of factors including: uptime, number of requests served, scheduled times during a day, memory (virtual or committed) used, and on-demand. By default, recycles are done in an overlapping fashion—the old process is not told to shutdown until the replacement process is ready to and starts serving requests.

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. IIS 6.0 features many new performance and scalability features, which include the following:

- **Kernel-mode Caching of Static and Dynamic Content.** The benefit to this feature is that many customers have programmatically created content that doesn't change. In previous versions of IIS, requests had to transition from kernel mode to user mode for every 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. In addition, dynamic responses can be cached within the kernel, also resulting in far fewer transitions to user mode, thus reducing the amount of time it takes to serve a request.
- **Large Memory Support for x86.0.** For workloads that require a great deal of cached data, IIS 6.0 can be configured to cache up to 64 gigabytes (GB) for an x86 system.
- **Caching Policy 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's scalability improves because it makes better use of the resources on the server while sustaining the performance on frequent requests.
- **Web Gardens.** A Web garden is an application pool that has multiple processes serving the requests routed to that pool simultaneously. 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. For example, if there are four processes in the Web garden and one process becomes blocked for some reason, there are three other processes available to handle the incoming requests.
- **Persisted ASP Template Cache.** Before Active Server Pages (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 time compiling it again.
- **Site Scalability.** IIS 6.0 has improved the way internal resources are used. The IIS 6.0 approach is much more one of allocating resources as HTTP requests request certain system resources, rather than pre-allocating resources at initialization time. This has resulted in the following improvements:
 - Many more sites that can be hosted on a single IIS 6.0 server.
 - A larger number of worker processes that can be concurrently active.
 - Quicker startup/shutdown of the server when hosting sites.
 - Listening for requests with no process running. An additional scalability improvement in the new IIS 6.0 architecture is that IIS can listen for requests from a large number of sites without having any worker processes running. (See [Request Processing Architecture](#) earlier in this paper). Coupling this "demand-start" feature with the ability to aggressively idle-out worker processes means that a Web server hosting many sites can be scaled further. This is because IIS 6.0 tunes its resource

use to the sites that are actually active. IIS 6.0 will also trim kernel cached items for these inactive sites dynamically.

Preliminary Testing Shows Significant Performance Increases

Initial testing of IIS 6 has shown the following performance results:

- Throughput increases of more than 100 percent over previous releases on a benchmark using an eight processor server. This gain is due to the new request processing architecture and scalability improvements in the Web application server.
- Throughput increases of up to 100 percent on an eight processor server, under particular workloads.
- Performance gains of 200 percent better throughput of static content and cached responses achieved up to 165 percent higher throughput when compared to IIS 5.0.
- Performance improvements of more than 50 percent higher throughput due to persistent on-disk caching.
- An order of magnitude greater number of pooled applications can be run on IIS 6.0 as compared to IIS 5.0. IIS 6.0 is capable of having thousands of isolated applications configured, and each of these applications can run with its own security identity. The number of concurrent isolated applications is a function of system resources. IIS 6.0 can easily have tens of thousands of configured applications per server, when applications are configured to execute in a shared application pool.
- Startup times for 20,000 sites are less than two minutes on a two processor server.

Securing IIS

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, improvements have been made to IIS to make it easier to further lock down a site and to discover and apply security patches. Security improvements include the following:

- **Locked Down Server.** To start with, IIS is not installed by default on clean installations, and disabled by default on upgrades.
- **IIS Web Services Extensions.** To reduce the attack surface of your Web server, IIS 6.0 serves only static content after a default installation. Programmatic functionality provided by IIS APIs (ISAPI) or Common Gateway Interfaces (CGI) must be manually enabled by an IIS administrator. Using the Web Service Extension node, Web site administrators can enable or disable IIS functionality based on the individual needs of the organization. Therefore, additional functionality such as Active Server Pages or FrontPage® Server extensions will have to be enabled before their functionality works as expected. IIS 6.0 provides programmatic, command-line, and graphical interfaces for enabling Web service extensions.
- **Configurable Worker Process Identity.** Running multiple applications or sites on one Web server puts additional requirements on a Web server. If an ISP hosts two companies, who may even be competitors, on one server, it has to guarantee that these two applications run completely isolated from each other. More importantly, the ISP has to make sure that a malicious attacker for one application can't access the data of the other application. Complete isolation is a must. IIS 6.0 provides this level of

isolation through the configurable worker process identity. Together with other isolation features, or memory-based recycling, IIS 6.0 provides an environment to host even the fiercest competitors on one Web server. Similarly, IIS 6.0 provides an environment to run multiple applications on one Web server with complete isolation.

- **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 ability to exploit a security vulnerability can be contained if the worker process has very few rights on the underlying system.
- **SSL Improvements.** There are three main secure sockets layer (SSL) improvements in IIS 6.0. They are:
 - **Performance.** IIS 5.0 already provides the fastest software-based SSL implementation on the market. As a result, 50 percent of all SSL Web sites run on IIS. IIS 6.0 will be even faster. Microsoft tuned and streamlined the underlying SSL implementation for even more performance and scalability.
 - **Remotable Certification Object.** In IIS 5.0, administrators cannot manage SSL certificates remotely because the cryptographic service provider (CAPI) certificate store is not remotable. Because customers manage hundreds or even thousands 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.** If SSL is enabled, performance drops dramatically because the CPU has to perform a lot of intensive cryptography. There are hardware-based accelerator cards that enable the offloading of these cryptographic computations to hardware. They plug their own Crypto API- (CAPI) provider into the system. IIS 6.0 makes it easy to select such a third-party provider.
- **Authorization and Authentication.** If authentication answers the question, “Who are you?” then authorization answers the question, “What can you do?” So authorization is about allowing or denying a user to conduct a certain operation or task. Windows Server 2003 integrates Passport as a supported authentication mechanism for IIS 6.0. IIS 6.0 extends the use of a new authorization framework that comes with the Windows Server 2003 family. Additionally, Web applications can use URL authorization in tandem with Authorization Manager to control access. Constrained, delegated authorization was added in Windows Server 2003 to provide domain administrators with control to allow delegation to particular machines and services only.
- **Passport Integration.** Windows Server 2003 integrates Passport as a supported authentication mechanism for IIS 6.0: This integration provides Passport authentication in the core Web server and uses Passport version 2 interfaces provided by standard Passport components. Administrators can take advantage of the Passport customer base of more than 150 million without having to deal with account management issues like password expiration or provisioning. Once Passport authentication is verified, a Windows Server 2003 Passport user can be mapped to a user of Active Directory through their Windows Server 2003 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 HTTP request. Application developers and Web site administrators can use this security model for authorization based on users of Active Directory. These credentials are also delegatable using the new Constrained Delegation feature that is supported in Windows Server 2003.

- **URL Authorization and Extending the New Authorization Framework.** Today, access control lists (ACLs) are used to make authorization decisions. The problem is that the ACL model is very object (file, directory) driven and tries to fulfill the requirements of the resource manager—the NTFS file system. But most Web applications used today are now business applications and are not object driven—they are operation- or task-based. If an application wants to provide an operation- or task-based access control model, it has to create its own. With the new authorization framework in Windows Server 2003, Microsoft provides a way to fulfill the needs of these business applications.
- **Constrained, Delegated Authentication.** Delegation is the act of allowing server applications to act as the user on the network. An example of this would be a Web service application on an enterprise intranet that accesses information from various other servers in the enterprise as the client, and then presents the consolidated data over HTTP to the user. Constrained delegation was added in Windows Server 2003 to provide domain administrators with control to allow delegation to particular computers and services only.

Managing IIS

The typical Internet Web site no longer operates on just one server. Web sites now spread across multiple Web servers, or across Web farms; (Web farms 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 and organizations are delivering more applications over the Web.

In addition, as remote administration has become more common, there has been an increasing demand for improved API access, and to improve direct 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 has become an integrated and complex process.

IIS 6.0 introduces new features to improve the administration capabilities for administrators who manage IIS Web sites. Management features include the following:

- **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 new XML metabase allows administrators to easily read and edit configuration directly without having to use scripts or code to administer the Web server.
- **Edit While Running.** Administrators can edit the XML metabase while the server is running.
- **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 Visual Basic® scripting language, 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.
- **Web Administration Console.** Using the Remote Administration (HTML) Tool, administrators are able to remotely administer IIS across the Internet or the intranet through a Web browser
- **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. The goal of the IIS WMI provider is to provide manageability of IIS at a level of functionality equivalent to the IIS ADSI provider and to support an extensible schema.

For more information about IIS, see [Technical Overview of Internet Information Services 6.0](#).

Server Consolidation

Consolidating multiple servers helps organizations lower total cost of ownership (TCO) while improving a wide range of areas that boost productivity including performance, scalability, manageability, availability, interoperability, and security. Targets for server consolidation in many organizations include the following:

- **File and Print Servers.** Features enabling file and print server consolidation include DFS improvements, improved File Replication Service (FRS), Dynamic Volume Management, NTFS journaling file system, Volume Shadow Copy service, Shadow Copy Restore, and Multipath I/O (MPIO), as explained earlier in this paper.
- **Line of Business Application Hosting.** Features enabling line of business application hosting include the Windows System Resource Manager (WSRM) and side-by-side DLL support, as explained in the section in this paper, [Side-By-Side Application Support](#).
- **Networking Servers.** This includes servers running directory services, DNS, WINS, and other core services. Features enabling networking consolidation include centralized management in Active Directory, ADMT, Application Directory Partitions, and Terminal Services, as explained earlier in this paper.
- **Web and Application Servers.** Features enabling Web and application server consolidation include worker process isolation, application pools, rapid fail protection, XML metabase, Web administration console, and Web gardens, as explained earlier in this paper.

Improving Availability

As you consolidate servers, each server will serve more users. This increases the focus on availability of servers. When running either Windows Server 2003, Enterprise Edition or Windows Server 2003, Datacenter Edition, you can consolidate your servers into clusters to provide high availability and scalability for mission-critical applications. High availability features include:

- **Eight-Node Clustering.** This allows up to eight servers to work together to run a common set of applications while providing the image of a single system to clients and applications. 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. This makes systems more highly available, scalable, and manageable, providing potential cost savings from reduced downtime.
- **Geographically Dispersed Clusters.** This enables you to increase availability by creating clusters in which the servers are located in different places. This helps ensure that availability will not be affected by events such as power outages or natural disasters. System administrators have more flexibility by being able to add and remove hardware in a geographically dispersed cluster, a benefit that also yields improved scaling options for applications.
- **SAN-Aware Clustering.** With storage area network (SAN)-aware clustering, administrators can centralize server storage into a SAN including boot, pagefile, and system disks using a single or multiple redundant HBAs. This allows administrators to take advantage of SANs and integrate clusters, leveraging existing investments and reducing system administration costs.

Enabling Interoperability

In addition to Windows NT 4.0, you may be running UNIX, NetWare, or mainframe operating systems on your network. Windows Services for UNIX (SFU) 3.0, an add-on service, provides a full range of cross-platform services that help you integrate Windows into your existing UNIX environments, for example by sharing data and management information such as user IDs and passwords. With Interix subsystem technology built in, Windows Services for UNIX 3.0 provides platform interoperability and application migration components in one fully integrated and supported product from Microsoft.

Microsoft Services for NetWare version 5, an add-on service, provides a complete set of new interoperability utilities that help Novell customers simplify the adoption of Windows Server 2003 into a Novell network environment, reduce multi-platform network administration, and facilitate the migration of NetWare resources to Windows 2000 Server.

Boosting Performance

Windows Server delivers significant performance improvements compared with Windows NT Server 4.0 on the same hardware. This enables IT professionals to reduce the number of servers needed to provide certain important services such as file and print. Features that improve performance for file systems include enhanced bandwidth throttling and better input/output (I/O) performance across disks. Internet Information Services 6.0 provides dramatically better performance compared with Internet Information Server 4.0 in Windows NT Server 4.0. Performance monitoring tools give administrators finely tuned information on a wide range of areas including disk input/output, memory management, drivers, pool allocations, heap allocations, and CPU.

Consolidating Application Servers: Side-By-Side Application Support

Side-by-side DLLs make application consolidation much easier by solving conflicts between applications that require different versions of the same DLL. Side-by-side DLLs enable application co-existence and improve system reliability. Together with the ability to support multiple Web applications in one instance of IIS, this is a basic technology enabler to consolidate applications on the same platform.

Windows System Resource Manager

The Windows System Resource Manager (WSRM) is a feature in both Windows Server 2003, Enterprise Edition and Datacenter Edition that allows an enterprise to consolidate multiple applications onto a single instance of Windows, while allocating server resources according to business priorities.

Policies are used to select the processes to be managed, and to set resource usage targets or limits. This helps avoid situations where applications contend for the same resources—for example, where one non-critical application might dominate the CPU and slow down responses to other more critical applications. Managed resources include: percent CPU utilization, process working set size (physical resident pages), and committed memory (for example, pagefile usage). WSRM also creates records for usage audits.

The ability to allocate resources addresses many business situations, including:

- **Server Consolidation.** The administrator can allocate resources to reduce the ability of applications to interfere with each other. This includes running multiple instances of a single application, and combining business-critical applications with other applications or services.

- **Managing Users.** Users can be managed by application in large terminal server systems—either individually or by security group. This prevents resource hogs.
- **Managing Resources.** WSRM enables administrators to manage the level of resources used by individual Internet Information Services 6.0 (IIS 6.0) application pools on a server, for example, in a situation where one machine hosts multiple Web sites.

Related Links

See the following resources for further information:

- [Top 10 Features for Organizations Upgrading from Windows NT 4.0 Server 4.0](http://www.microsoft.com/windowsserver2003/evaluation/whyupgrade/top10nt.mspx) at <http://www.microsoft.com/windowsserver2003/evaluation/whyupgrade/top10nt.mspx>.
- [Top 10 Features for Organizations Upgrading from Windows 2000 Server](http://www.microsoft.com/windowsserver2003/evaluation/whyupgrade/top10w2k.mspx) at <http://www.microsoft.com/windowsserver2003/evaluation/whyupgrade/top10w2k.mspx>.
- [Technical Overview of Internet Information Services 6.0](http://www.microsoft.com/windowsserver2003/techinfo/overview/iis.mspx) at <http://www.microsoft.com/windowsserver2003/techinfo/overview/iis.mspx>.
- [Using the Application Compatibility Toolkit](http://www.microsoft.com/windowsserver2003/compatible/appcompat.mspx) at <http://www.microsoft.com/windowsserver2003/compatible/appcompat.mspx>.

For the latest information about Windows Server 2003, see the [Windows Server 2003 Web site](http://www.microsoft.com/windowsserver2003) at <http://www.microsoft.com/windowsserver2003>.