

iTCo

New in Windows
2003

White Paper

Table of Contents

Table of Contents.....	1
Active Directory	2
Application Services	3
Clustering Technologies	5
File and Print Services	7
Internet Information Services 6.0.....	9
Management Services.....	10
Networking and Communications	12
Security	14
Storage Management	15
Terminal Server.....	17
Windows Media Services	17
Enterprise UDDI Services	18

Active Directory

Feature	Description
ADMT version 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 Microsoft Windows NT® 4.0 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.
AD/AM	Active Directory in Application Mode (AD/AM) is a new capability 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. Note: AD/AM will be released as a separate component with Windows Server 2003.
Group Policy Improvements	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.
Enhanced UI	As the principal means to manage enterprise identities, objects, and relationships, improved interfaces increase administration efficiency and integration capabilities. Microsoft Management Console (MMC) plug-ins now include drag-and-drop capabilities, multi-object selection, and the ability to save and reuse queries. Administrators may now edit multiple user objects simultaneously, reset access control list (ACL) permissions to the default, show effective permissions on a security principal, and indicate the parent of an inherited permission.
Cross-Forest Authentication	Cross-forest authentication enables secure access to resources when the user account is in one forest and the computer account is in another forest. This feature allows users to 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.
Cross-Forest Authorization	Cross-forest authorization makes it easy for administrators to select users and groups from trusted forests for inclusion in local groups or ACLs. This feature maintains the integrity of the forest security boundary while allowing trust between forests. It enables the trusting forest to enforce constraints on what security identifiers (SIDs) it will accept when users from trusted forests attempt to access protected resources.
Cross-Certification Enhancements	The Windows Server 2003 client cross-certification feature is enhanced by enabling the capability for department-level and global-level cross certifications. For example, WinLogon will now be able to query for cross certificates and download these into the "enterprise trust/enterprise store." As a chain is built, all cross certificates will be downloaded.
IAS and Cross-Forest Authentication	If Active Directory forests are in cross-forest mode with two-way trusts, then Internet Authentication Service/Remote Authentication Dial-In User Service (IAS/RADIUS) can authenticate the user account in the other forest with this feature. This gives administrators the capability to easily integrate new forests with already existing IAS/RADIUS services in their forest.
Credential Manager	The Credential Manager provides a secure store of user credentials, including passwords and X.509 certificates. This will provide a consistent single-sign on experience for users, including roaming users. For example, when a user accesses a line-of-business application within their company's network, the first attempt to access this application requires authentication and the user is prompted to supply a credential. After the user provides this

	credential, it will be associated with the requesting application. In future access to this application, the saved credential will be re-used without prompting the user.
Software Restriction Policies	Software restriction policies address the need to regulate unknown or untrusted software. With software restriction policies, you can protect your computing environment from untrusted software by identifying and specifying which software is allowed to run. You can define a default security level of unrestricted or disallowed for a GPO so that software is either allowed or not allowed to run by default. You can make exceptions to this default security level by creating rules for specific software.
Easier Logon for Remote Offices	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 (WANs). The loss of connectivity between a branch office and a global catalog no longer impacts the ability of branch users to log on. Branch offices can be supported more effectively and bandwidth consumption over WAN links is reduced.
Group Membership Replication Enhancements	As group members are added, changed, or deleted, only the changes are replicated, a benefit that reduces the burden on network bandwidth and processor usage. This largely eliminates the possibility of lost updates during simultaneous updates.
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.
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 domain controller or global catalog server.
Dependability Improvements	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.

Application Services

Feature	Description
Native XML Web Services Support	Windows Server 2003 offers native support for XML Web service standards including XML, SOAP, Universal Description, Discovery and Integration (UDDI), and Web Services Description Language (WSDL).
Enterprise UDDI	Windows Server 2003 includes Enterprise UDDI Services, dynamic and flexible infrastructure for XML Web services. This service enables companies to run their own internal UDDI service for intranet or extranet use. 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. With UDDI Services, companies can build and deploy smarter, more reliable applications.
Support for Existing Services	Because XML Web services are deeply integrated into Windows Server 2003, existing services like COM+ and Microsoft Message Queuing (MSMQ) can readily take advantage of them. Administrators can allow existing COM+ applications to be called using XML/SOAP by simply checking a configuration box. MSMQ can also talk to SOAP and XML as a native format to allow loosely coupled applications to interoperate with a broad range of systems.
Federation Infrastructure	XML Web services deliver the foundation and architecture for application integration. Federation infrastructure is fundamentally about enabling servers and services to interoperate across trust boundaries.
Microsoft .NET Framework	<p>The .NET Framework incorporates the common language runtime and a unified set of class libraries that include Windows Forms, Microsoft ADO.NET, Microsoft ASP.NET, and other capabilities.</p> <p>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.</p> <p>By integrating the .NET Framework into the Windows Server 2003 application development environment, developers are freed from writing "plumbing" code and can instead focus their efforts on delivering real business value.</p> <p>The .NET Framework which Windows XP, Windows 2000 Server and Windows 2000</p>

	<p>Professional, Windows 98, Windows Me, and Microsoft Windows NT® 4.0 all supportenables 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.</p> <p>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 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.</p>
ASP.NET: Simple Web Service Creation	Using the ASP.NET XML Web services features, developers can write their business logic and the ASP.NET infrastructure will be responsible for delivering that service via 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.
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.
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.
ASP.NET: Integrated with Internet Information Services (IIS) 6.0	ASP.NET is integrated with the 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: 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 which 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 application programming interface (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.
Garbage-collected Environment	The garbage collector in the common language runtime provides a more efficient environment for memory management in Web server scenarios. It avoids heap fragmentation issues by using a classic allocation/free model.
Asynchronous Support	The .NET Framework deeply integrates two asynchronous communication technologies for scalability and reliability: SOAP and 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 machines in a Web farm.
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.

Clustering Technologies

Feature	Description
Easy Setup and Configuration	<p>The cluster service is an integral part of the Windows 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 Administration tools from a remote management station. No reboots are required to set up a server cluster configuration.</p> <p>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.</p> <p>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 administration tools.</p> <p>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.</p>
Larger Clusters Now Supported	<p>In Datacenter Edition, the maximum supported cluster size has been increased from 4-nodes in Windows 2000, to 8-nodes in Windows Server 2003.</p> <p>In Enterprise Edition, the maximum supported cluster size has been increased from 2-nodes in Windows 2000 Advanced Server to 8-nodes in Windows Server 2003.</p> <p>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 more flexibility in building multi-site, geographically dispersed clusters that provide for disaster tolerance, as well as traditional node and/or application failure.</p>
Integrates with Active Directory Service	<p>Server clusters running Windows Server 2003, 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.</p>
64-Bit Support	<p>Server clusters are fully supported on computers running the 64-bit versions of Windows Server 2003. Applications that can take advantage of the increased memory space of computers running the 64-bit versions of Windows Server 2003 can also take advantage of the high availability offered by failover.</p>
Increased Manageability	<p>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.</p>
Easy Resource Configuration	<p>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.</p> <p>Applications can be made server 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.</p> <p>Resource-specific properties are also supported; this allows resource scripts to be used to store server cluster-wide configuration information which 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.</p>
Network	<p>Server clusters take advantage of important network enhancements. Enhanced logic for</p>

Enhancements	<p>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.</p> <p>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. Multi-cast heartbeats is automatically selected—if a server cluster is large enough, and the network infrastructure can support multi-cast between the cluster nodes. If multicast communication fails for any reason, internal communications revert to unicast. In any event, all internal communications are signed and secure.</p>
Improved Storage Capabilities	<p>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.</p> <p>The improved Distributed File System (DFS) now includes: multiple standalone roots, independent root failover, support for active/active configurations, and allows multiple file shares on different machines to be aggregated into a common namespace.</p> <p>Clustering Services has been optimized for storage area networks (SAN), including targeted device resets and storage interconnect requirements.</p> <p>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.</p>
Streamlined Operation	<p>Server clusters take advantage of important operational capabilities. Databases and configuration data can be backed up and restored, while enhanced node failover supports failover for clusters with three or more nodes. Group affinity support provides improved performance and availability because applications are failed over to spare nodes before active nodes.</p> <p>Rolling upgrades from Windows 2000 to the Windows 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.</p> <p>Resource deletions are done using Cluster Administrator or with Cluster.exe, without having to take the resource offline. Windows Management Instrumentation (WMI) support is provided in the following areas: cluster control and management, application and cluster state information, and cluster state change events.</p>
Easier Troubleshooting and Failure Recovery	<p>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.</p> <p>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.</p> <p>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.</p>
New Cluster Topologies	<p>Windows 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.</p>
EFS is Supported on Clustered Disks	<p>Windows Server 2003 supports Encrypting File System (EFS) on clustered (shared) disks.</p>
Network Load Balancing Manager	<p>This new utility in Windows Server 2003 provides a single point of configuration and management for NLB clusters. NLB Manager can be used to:</p>

	<ul style="list-style-type: none"> • 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 server cluster IP 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.
Virtual Clusters	<p>This new feature in the Windows Server 2003 can be used to:</p> <ul style="list-style-type: none"> • 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	<p>The Windows Server 2003 binds NLB to multiple network cards and enables users to:</p> <ul style="list-style-type: none"> ▪ 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	<p>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 Web publishing and server publishing. While Web publishing does not require bi-directional affinity, server publishing does. 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.</p>
Internet Group Management Protocol (IGMP) Support	<p>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.)</p> <p>IGMP-support conserves network resources by limiting flooding to only those ports on a switch that have NLB machines connected to them. Note: IGMP-support can only be enabled when NLB is configured in multicast mode.</p>

File and Print Services

Feature	Description
Remote Document Sharing (WebDAV)	A new feature in Windows 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.
Automated System Recovery (ASR)	A new feature in Windows Server 2003, ASR improves productivity by enabling one-step restore of operating system, system state, and hardware configuration in disaster recovery situations.
Command-line Interface	Windows 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 Windows Server 2003, support a new disk partitioning style, the 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 availability and performance by optimizing files on a volume. Defrag in Windows Server 2003 is faster and more efficient than it was in Windows 2000. Plus it supports online defrag of the Master File Table (MFT) and can defrag NTFS volumes with any cluster size.
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 System (DFS)	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 and administration can be delegated. In Windows 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 Server 2003 system can host multiple DFS roots.
DFS File Replication Services (FRS)	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 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)	EFS complements other access controls providing an added level of protection for your data. EFS runs as an integrated system service, making it easy for you to manage, difficult to attack, and transparent to the user.
New Support for Antivirus Products	A new feature in Windows Server 2003, this includes 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. If, in the unlikely event a disk does need to be checked (less than 1 percent of unplanned outages require such checking), CHKDSK performs between 20 percent and 38 percent faster than it did in Windows 2000.
Shadow Copies for Users	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.

Command-line Interface	Windows Server 2003 provides new command-line utilities for many print management tasks including printer management and configuration, job and queue control, port management, and driver management.
Print Cluster Support (Enterprise Edition & Datacenter Edition only)	This feature improves productivity by making it easier to install printer drivers on server clusters. When installing a printer driver on a virtual cluster, Windows Server 2003 automatically propagates the driver to all nodes of the cluster.
64-Bit Printing Support	This feature provides support for 64-bit drivers and applications. "Point-n-print" provides client-server printing support for interoperability of 32-bit to 64-bit clients and servers.
Wide Range of Devices	Windows Server 2003 improves connectivity with built-in support for more than 3,800 new printer drivers.
Reliability Improvements	Windows 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, you can 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 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 Server 2003 improves your productivity by recognizing and adapting to hardware configuration changes automatically.
Easier Printer Management	You can easily monitor operation of local and remote printers. With System Monitor you 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 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, a benefit that simplifies printing across a network and saves 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.

Internet Information Services 6.0

Feature	Description
New Request-Processing Architecture	With the new request-processing architecture, IIS 6.0 automatically detects memory leaks, access violations, and other errors. When these conditions occur, the underlying architecture provides fault tolerance and the ability to restart processes as necessary. Meanwhile, IIS 6.0 continues to queue requests without interrupting the user experience.
Health Detection	IIS 6.0 is capable of monitoring the health of worker processes, applications, and Web sites. It can detect the status of worker process as well as recycle worker processes based on various factors including uptime, a designated schedule, number of requests, and memory consumption. Or it can recycle worker processes on demand.
Site Scalability	IIS 6.0 has improved the way the operating system uses internal resources. For example, IIS 6.0 does not pre-allocate resources at initialization time. Many more sites can be hosted on a single server running IIS 6.0, and a larger number of worker processes can be concurrently active. Starting up and shutting down a server is faster compared with earlier versions of IIS. All of these improvements contribute to increased site scalability with IIS 6.0.
New Kernel Mode Driver, HTTP.SYS	Windows Server 2003 introduces a new kernel mode driver, HTTP.SYS, for HTTP parsing and caching, providing increased scalability and performance. IIS 6.0 is built on top of HTTP.SYS and is specifically tuned to increase Web server throughput. In addition, HTTP.SYS directly processes requests in the kernel under specific circumstances.
Locked-down Server	IIS 6.0 provides significantly improved security. To reduce the attack surface of systems, IIS 6.0 is not installed by default on Windows Server 2003: administrators must explicitly select and install it. IIS 6.0 ships in a locked-down state, serving only static content. Using the Web service extension node, Web site administrators can enable or disable IIS functionality based on the individual needs of the organization.
Authorization	IIS 6.0 extends the use of a new authorization framework that comes with Windows Server 2003. In addition, Web applications can use URL authorization—in tandem with

	Authorization Manager—to control access. Constrained, delegated authorization now provides domain administrators with control to delegate only to particular computers and services.
XML Metabase	The XML-formatted, plain-text metabase in IIS 6.0 provides improved backup and restore capabilities for servers that experience critical failures. It also provides for improved troubleshooting and metabase corruption recovery. Direct editing, using common text editing tools, provides greater manageability.
ASP.NET and IIS Integration	Windows Server 2003 offers an improved developer experience with Microsoft ASP.NET and IIS integration. Building on IIS 6.0, Windows Server 2003 enhancements offer developers very high levels of functionality, such as rapid application development (RAD) and a broad choice of languages. In Windows Server 2003, the experience of using ASP.NET and the Microsoft .NET Framework is improved because the request-processing architecture is integrated with IIS 6.0.
Share Information Across Geographical Boundaries	Sharing information across geographical boundaries, in a variety of languages, is becoming more important in a global economy. In the past, the non-Unicode structure of the HTTP protocol limited developers to the system codepage. Now, with URLs encoded by Unicode Transformation Format-8 (UTF-8), Unicode becomes possible, a benefit that provides the capability to support more complex languages such as Chinese. IIS 6.0 allows customers to access server variables in Unicode. It also adds new server support functions that allow developers access to the Unicode representation of a URL, thereby improving international support.

Management Services

Feature	Description
Group Policy Management Console	<p>Expected to be freely available as an add-in component, the Group Policy Management Console (GPMC) provides 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 management features.</p> <p>For example, GPMC enables backup and restore of Group Policy objects (GPOs), import/export and copy/paste of GPOs, reporting of GPO settings and RSoP data, use of templates for managed configurations, and scriptability for all GPMC operations. In addition, GPMC lets administrators manage Group Policy for multiple domains and sites within a given forest, all in a simplified user interface 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 Server 2003 domains.</p>
Resultant Set of Policy (RSoP)	The Microsoft RSoP tool provides administrators with a powerful and flexible base-level tool to plan, monitor, and troubleshoot Group Policy. With RSoP, administrators can plan how Group Policy changes would affect a targeted user or computer. Or administrators can remotely verify the policies currently in effect on a specific computer.
New Policy Settings	With more than 200 new policy settings for Windows Server 2003, organizations can easily lock down or manage configurations such as customizing or prohibiting hundreds of features like Remote Assistance, AutoUpdating, and Error Reporting.
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	WMI filtering lets administrators determine whether to apply a GPO to a specific computer or user based on their configuration, role, or other criteria. For example, the use of Internet Protocol Security (IPSec) could be limited to only those machines that have a network interface card (NIC) optimized for it.
Cross-Forest Support	While GPOs can only be linked to sites, domains, or organizational units (OUs) within a given forest, the cross-forest feature in Windows Server 2003 enables several new scenarios that Group Policy supports. 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. Windows Server 2003 Group Policy successfully supports these interoperability scenarios.
User Data and	Administrators can automatically configure client computers to meet specific requirements

Settings Management Enhancements	of a user's business roles, group memberships, and location. Improvements include simplified folder redirection and more robust roaming capabilities.
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.
Remote Installation Services (RIS)	Administrators can use RIS servers using Risetup and RIPrep to deploy all editions of Windows 2000, Windows XP Professional, and all editions of Windows Server 2003 (except Windows 2000 Datacenter Server and Windows Server 2003, Datacenter Edition.) In addition, administrators can use RIS servers using Risetup to deploy Windows XP 64-bit Edition and the 64-bit versions of Windows Server 2003. Automated deployment is further enhanced with tighter security, improved performance to major components in RIS, such as Trivial File Transfer Protocol (TFTP), and hardware abstraction layer (HAL) filtering to ensure that images are recognized only by machines with a compatible 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.
User State Migration	Migrating files and settings for multiple users in a corporate environment is made easier with the User State Migration Tool (USMT). USMT gives administrators command-line precision in customizing specific settings such as unique modifications to the registry. In addition, Windows Server 2003 includes a Files and Settings Transfer Wizard designed for individual users or small office users. The wizard is also useful in a corporate network environment for employees who get a new computer and need to migrate their own files and settings without the support of an IT department or help desk.
Windows Installer	Managing software applications in a corporate environment has traditionally burdened organizations with high costs. Now with Windows Installer, administrators can 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 run time. The result: significantly lower TCO for managing applications.
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 via 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 (WMIC) 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.
Microsoft Windows Update Services Catalog Site	Administrators can download specific patches and drivers for distribution via Systems Management Server or other management tools.
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 via Group Policy.
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 provides administrators with greater control of updates. Automatic updates can be configured automatically over the Internet or administered in-house.
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 Windows Server 2003 product CD.
Driver Services	Windows 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.
Microsoft Software Update Services	Since many corporations do not want their systems or users going to an external source for updates without first testing these updates, Microsoft is providing an installable version of

	<p>Windows Update for inside your corporate firewall. Microsoft Software Update Services allows customers to install a service on an internal server running Windows 2000 Server or Windows Server 2003 that can download all "critical" updates as they are posted to Windows Update.</p> <p>Administrators will also receive e-mail 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.</p> <p>Client machines require the new Automatic Updates client, and can be configured centrally using Group Policy to automatically download and install approved updates.</p>
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.

Networking and Communications

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 driver provided with Windows Server 2003 is production quality and includes utilities, extensive API support (Windows Sockets, remote procedure call [RPC], and IPHelper), and IPv6-enabled system components such as Microsoft Internet Explorer, Telnet client, FTP client, Microsoft Internet Information Services (IIS) 6.0, file and print sharing, and others. IPv6 for Windows Server 2003 also provides support for IPv6/IPv4 coexistence technologies such as 6to4 and Intra-site Automatic Tunnel Addressing Protocol (ISATAP).
Point-to-Point Protocol over Ethernet (PPPoE)	Windows Server 2003 delivers a native PPPoE driver for making broadband connections to certain Internet service providers (ISPs) without the need for additional software. Small businesses or corporate branch offices may also utilize PPPoE's demand dial capabilities to integrate with the Routing and Remote Access service and NAT.
Network Bridging	Network bridging allows administrators to interconnect network segments using computers running Windows Server 2003. In a multi-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 network segments to communicate with each other through the bridge or communicate with the Internet when Internet Connection Sharing (ICS) is enabled.
Internet Protocol Security (IPSec) over NAT	The difficulty of using IPSec-based VPNs or IPSec-protected applications across a NAT is eliminated. Windows Server 2003 allows a Layer Two Tunneling Protocol (L2TP) over IPSec (L2TP/IPSec) or an IPSec connection to pass through a NAT. This capability is based on the latest IETF standards work. An administrator may also use this feature to secure perimeter network Microsoft Exchange Server traffic to an internal network running Exchange Server or a perimeter network application server to a partner's application server on the Internet without requiring a VPN server.
Additions to Group Policy	New Group Policy improvements in Windows Server 2003 give administrators granular control over most network configuration settings. For example, administrators may now configure some DNS client settings on computers running Windows Server 2003 using Group Policy. Furthermore, the Group Policy feature may be used to allow or restrict user configuration access to individual components of the network user interface.
Enhanced Connection Manager Administration Kit (CMAK)	<p>CMAK gives administrators the ability to predefine connection profiles for remote access users running Windows XP, Windows 2000, Microsoft Windows NT® 4.0, Windows Millennium Edition (Windows Me), and Windows 98.</p> <p>Windows Server 2003 delivers new features and improvements for CMAK, allowing administrators to provide more than one VPN server for connections, turn on end-user logging, automatically configure browser proxy settings on client computers, enable or</p>

	<p>disable client-side split tunneling, and configure pre-shared keys for L2TP/IPSec connections. The split tunneling feature permits client-side VPN connections to route corporate-based traffic over the VPN connection while isolating Internet-based traffic to the user's local Internet connection, thereby avoiding the use of corporate bandwidth for access to Internet sites. Security-sensitive companies can choose to use the default non-split model to ensure all client communications for VPN clients are protected by the corporate firewall.</p>
IAS Enhancements	<p>Wireless network deployments dramatically increase demand for multiple Remote Authentication Dial-In User Service (RADIUS) servers and better tools to diagnose authentication issues and manage network access control.</p> <p>Windows Server 2003 addresses this with new features that allow IAS to send RADIUS logging information to a server running Microsoft 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, Windows Server 2003 makes it easier to deploy high-scale solutions for authenticated network access control in wired, wireless, and remote access scenarios.</p>
Management and Integration Extensions	<p>The Windows Server 2003 family delivers exciting new networking features for simplifying the management of your enterprise network.</p> <p>A new Network Load Balancing Manager provides a single point of configuration and management for load balancing. Support for RFC 2734 allows TCP/IP traffic on an IEEE 1394 serial bus. Furthering our commitment to security, Windows Server 2003 provides support for the 2048-bit Diffie-Hellman group. This group provides a stronger Diffie-Hellman key exchange, allowing for the derivation of stronger secret keys.</p>
Internet Connection Firewall (ICF)	<p>ICF, designed for use in a small business, provides basic protection on computers directly connected to the Internet or on local area network (LAN) segments. ICF is available for LAN, dial-up, VPN, or PPPoE connections. ICF integrates with ICS or with the Routing and Remote Access service.</p>
IPSec Network Load Balancing	<p>Network Load Balancing provided with Windows Server 2003 now supports IPSec traffic. Administrators can use Network Load Balancing 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.</p>
Network Access Security with 802.1X	<p>Companies can move to a security model that ensures all physical access is authenticated and encrypted, based on the 802.1X support in Windows Server 2003. Using 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.</p> <p>Because 802.1X provides dynamic key determination, 802.1X wireless network encryption is dramatically improved by addressing many of the known issues associated with wired equivalent privacy (WEP) used by IEEE 802.11 networks.</p> <p>Using the Protected Extensible Authentication Protocol (PEAP), as authored by Microsoft in an IETF Internet draft, 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 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.</p>
IAS RADIUS Proxy and Load Balancing	<p>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.</p>

Security

Feature	Description
Internet Connection Firewall	Windows Server 2003 will provide Internet security using a software-based firewall called Internet Connection Firewall (ICF). ICF provides protection to computers directly connected to the Internet, or to computers located behind an Internet Connection Sharing (ICS) host computer that is running ICF.
Secure IAS/RADIUS Server	The Internet Authentication Server (IAS) is a Remote Authentication Dial-in User Server (RADIUS) that manages user authentication and authorization. It also manages connections to the network using a variety of connectivity technologies, such as dial-up, virtual private networks (VPNs), and firewalls.
Secure Wireless and Ethernet LANs	Windows Server 2003 enables the authentication and authorization of users and computers that connect to wireless and Ethernet LANs. This is accomplished by Windows Server 2003 support of the IEEE 802.1X protocols. (IEEE 802 standards define methods for accessing and controlling LANs.)
Software Restriction Policies	Windows Server 2003 will let a system administrator use policy or execution enforcement to prevent executable programs from running on a computer. For example, specific corporate-wide applications can be restricted from running unless they're executed from a particular directory. Software restriction policies can also be configured to prevent virus-infected or malicious code from running.
Security Improvements for Servers on Ethernet and Wireless LANs	Windows Server 2003 will provide security for both Ethernet and wireless LANs that are based on IEEE 802.11 specifications, and that support public certificates deployed using autoenrollment or smart cards. These security improvements enable access control to Ethernet networks in public places like malls or airports. Authentication of computers within an extensible authentication protocol (EAP) operating environment is also supported.
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. This feature supports the encryption and decryption of the entire offline database. 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: <ul style="list-style-type: none"> • L2TP (Layer Two Tunneling Protocol)/IPSec VPN client and server. • L2TP/IPSec tunnels for 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 Server (IIS) and the Active Directory® service.
System Security Improvements	Important improvements have been made to ensure overall system security including: <ul style="list-style-type: none"> • 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 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 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.
Certificate Autoenrollment and Autorenewal	These important new features dramatically reduce the amount of resources needed to manage X.509 certificates. Windows 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.
Certificate Revocation List (CRL) Improvements	The certificate server included in Windows Server 2003 now supports delta 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.
Passport Integration	A Passport identity can be mapped to an Active Directory identity within Windows 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 logon directly to a Windows network. Passport integration will provide an equivalent single sign-on experience using IIS.
Cross-Forest Trusts	If you're working with a partner or company that has an Active Directory forest deployed, you can use Windows 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.

Storage Management

Feature	Description
Multivendor Storage Management— Virtual Disk Service (VDS)	Virtual Disk service (VDS) enables multivendor storage devices to interoperate in Windows. VDS has APIs to storage hardware and to management programs that manage the storage hardware. Administrators can discover multivendor storage devices and configure those resources with a unified interface. Without VDS, each vendor's storage device often had its own management interface, resulting in many management interfaces in a mixed storage environment.
Data Management— Volume Shadow Copy Service	The Volume Shadow Copy service provides an infrastructure for creating a point-in-time copy of a single volume or multiple volumes. Used for managing data from direct attached storage to SANs, the Volume Shadow Copy service coordinates with business applications, backup applications, and storage hardware to enable application-aware data management. Solutions built on the Volume Shadow Copy service can produce much higher quality shadow copies than other technologies because of the ability to integrate with business applications and coordinate with storage hardware. As a result, high-fidelity backup recovery and data mining are possible without significantly affecting performance. In addition, the shadow copy restore feature enables Windows-based client computers to view and recover previous versions of their files without IT intervention, resulting in greater productivity at lower costs.
Data Protection— Encrypting File	The Encrypting File System (EFS) 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

System	<p>or folder—transparent to authorized users but inaccessible to anyone else.</p> <p>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.</p> <p>EFS improvements in Windows 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.</p>
Data Protection— Automated System Recovery	<p>Automated System Recovery (ASR) enables bare metal restore of servers and consistent data recovery of servers, including "system state" and hardware configuration information. Using recovery mode, ASR ensures a server can be returned to its original state if a serious failure occurs.</p> <p>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.</p>
Availability— Multipath I/O	<p>Multipathing is a high availability function that provides multiple paths from the host to the external storage device. Although multipath I/O (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.</p>
Open File Backup	<p>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 that any open files being accessed by users are also backed up.</p>
Improved Check Disk Command	<p>In Windows Server 2003, the performance of the Check Disk command, known as CHKDSK.exe, is between 20 percent and 38 percent faster than the version released with Windows 2000.</p> <p>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 Server 2003 will also be available for Windows 2000 Server.</p>
Storage Area Network Support	<p>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 2003.</p>
DISKPART Command	<p>The DISKPART.exe command-line program provides all the functionality of the Disk Manager Microsoft Management Console (MMC) Snap-in, but via the command line.</p> <p>In addition, DISKPART enables storage administrators to expand basic disks, a disk type used by Microsoft Cluster Services, as more disk space is required.</p>
Distributed File	<p>The Distributed File System (DFS) eases locating and managing data on your network. DFS</p>

System Improvements	<p>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.</p> <p>DFS is enhanced for Windows Server 2003, Enterprise Edition and Windows Server, 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.</p>
----------------------------	---

Terminal Server

Feature	Description
Increased Scalability	Enterprises need the ability to scale-up and scale-out. Terminal Server supports more users on each high-end server than Windows 2000; and Session Directory in Windows Server 2003, Enterprise Edition provides support for Microsoft's network load balancing and other third-party load balancing technologies.
Improved Manageability	Terminal Server 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.
Enhanced Remote Desktop Protocol (RDP)	When connecting to a terminal server 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 Server to support store kiosks displaying merchandise. They can be set to provide true color images for the best product image.
Additional Windows Server 2003 Enhancements	Terminal Server takes advantage of many Windows Server 2003 features, such as software restriction policies, roaming profile enhancements, and new application compatibility modes.

Windows Media Services

Feature	Description
Instant-on	
Fast Start	Provides an instant-on playback experience—no buffering delay—whether playing a single piece of content, or switching seamlessly between on-demand clips or broadcast channels.
Always-on	
Fast Cache	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	Virtually eliminates packet corruption and interruption over high latency network connections—for example wireless and satellite—using local packet correction. This ensures

	an uninterrupted viewing experience.
Fast Reconnect	Automatically restores live or on-demand player/server and server/server connections if disconnected during a broadcast. This ensures an uninterrupted viewing experience.
Server-side Playlists	Whether on-demand or live, server-side playlists provide the unprecedented ability to dynamically change content within a playlist during broadcasts, without interrupting the viewer. For example, you can change the order of clips, insert a new clip, insert an ad, and others.
Automatic Playlist Generation	Personalized playlists can be programmed on the server and sent to a wireless device. This increases the reach of playlist distribution to include wireless devices.
Ad Insertion	A wide variety of advertising types are supported, including lead-ins and interstitials. Windows Media Services integrates with third party ad servers and includes advanced usage reporting.
More Scalable	Twice as many concurrent users can be supported. This enables streaming for the largest enterprises and content distribution networks.
More Reliable	Plug-ins run in protected memory, ensuring maximum system reliability.
Cache/Proxy Platform	Developers can 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.
Flexible Administration Tools	Flexible administration—using Microsoft Management Console (MMC), Web browser, or command-line scripts—enables server management in virtually any environment.
Scenario-based Wizards and Help	Wizards ease the set-up and configuration of common management activities. The help system is improved and organized around common audio and video streaming scenarios.
Secure Content Delivery	Content is securely distributed from server-to-server and server-to-client using a variety of common authentication and authorization mechanisms, including new support for HTTP Digest. Digital rights management for on-the-wire and persistent client-side security is also supported.
Standards-based	Support for HTTP 1.0/1.1, RTP, RPSP, HTML v3.2, FEC; IPv4/6, IGMPv3, SNMP, WEBM/WMI, SMIL 2.0, SML, SML-DOM, and COM/DCOM provide maximized streaming capabilities and integration.
Flexible Plug-in Interfaces	Developers can easily extend Windows Media Services functionality to integrate existing systems and solutions, such as storage systems, billing, and logging applications.
Powerful Object Model and Event Mechanism	Developers can easily build custom applications for configuring and monitoring Windows Media Services. This is done using standard WBEM/WMI, and the industry's most extensive object model with over 700 server interfaces.
Broad Programming Language Support	Developers can write plug-ins and custom applications using a programming language they are already familiar with, such as C++, C#, VB Script, or Perl.

Enterprise UDDI Services

Feature	Description
Enterprise UDDI Services	<p>Built as a managed code service in Windows Server 2003, Enterprise UDDI Services was developed using Microsoft ASP.NET and the Microsoft .NET Framework. It is a standards-based technology that takes advantage of Microsoft's own experience in running the Microsoft public node of the UDDI Business Registry (UBR). UDDI Services can be accessed through a Web-based user interface or programmatically through a SOAP interface.</p> <p>Because UDDI Services automatically publishes its existence and location, it is easily discoverable as a Web service. UDDI Services is available in Windows Server 2003, Standard Edition, Enterprise Edition, and Datacenter Edition.</p>
Active Directory Integration	UDDI Services takes advantage of many features in the Active Directory® service. 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 means for finding servers on the network that run UDDI Services. In addition, UDDI Services can optionally be installed as a service within Active Directory, enabling IT administrators, users, or applications to perform a simple query to obtain a list of all UDDI Services on the network.
UDDI Application Programming Interface (API) and	UDDI Services supports programmatic inquiries through the UDDI API and also includes a 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

Web-based User Interface	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 and Publication	Authorized users can query UDDI Services and publish entries using the Web-based user interface or the UDDI API.
Coordinator Role	Microsoft has added the coordinator role to provide enhanced administrative capabilities.
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 software development kit (SDK). Visual Studio .NET provides native support for UDDI Services through the command "Add Web Reference" enabling developers to easily discover Web services and other programmatic resources in UDDI for use in building applications.
Data Import	A UDDI Services coordinator can import UDDI data from an XML file that complies with a defined schema.
Authentication	UDDI Services supports native UDDI authentication and native Windows authentication.
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: user, publisher, coordinator, and administrator.
Microsoft Management Console (MMC) Administration Utility	UDDI Services site administrators can easily configure and remotely administer the UDDI Services server by using the Microsoft Management Console (MMC) utility. Site administrators can backup and restore the UDDI Services database.
Database and Server Configuration	UDDI Services uses the Microsoft Data Engine as the default store. For high reliability and availability scenarios, UDDI Services can use Microsoft SQL Server 2000. UDDI Services may be deployed on a single server or across multiple servers. For example, IT administrators could distribute the Web-based user interface and APIs across one or more servers in a typical Web farm configuration and run the database on a separate dedicated server running SQL Server 2000. Or IT administrators could run the database on a clustered instance of SQL Server 2000 using Microsoft's clustering technology configuration that provides great scalability and reliability.
Activity Monitoring	Windows Server 2003 provides the ability to audit all authenticated activities performed and the user that performed them.

Simplify IT
iTCO
your eBusiness Partner
www.itcosolutions.com

iTCO Solutions Corporation
P.O. Box 610090
Redwood City, CA 94061
United States

<http://www.itcosolutions.com/>

Enterprise Sales Team Contact
Ryan Edwards
National Accounts Manger
Tel: 650-367-0514
E-Mail: redwards@itcosolutions.com