

Microsoft White Paper



LEGATO NetWorker and Windows Server 2003™

Microsoft®

INTRODUCTION	3
WINDOWS SERVER 2003 – AN OVERVIEW	5
Improvements across the board	5
FEATURES AND BENEFITS	5
Security	5
Internet Information Services 6.0	8
Scalability	8
Reliability and Availability	10
Manageability	11
LEGATO NETWORKER 7.1	14
Removable Storage Support	14
Volume Shadow Copy Service Support	14
NetWorker DiskBackup	15
Automated System Recovery Support	15
Cluster Awareness	15
64-bit Version Support	16
TapeAlert Capability	16
Unique Identification of Devices	16
Service Mode for Devices	16
Improved Error Handling for Lost Volume Names	16
User Group Resource	17
Monitoring NetWorker Resources	17
Generating Program-Readable Reports	17
Comment Attribute in NetWorker Resources	18
User Identification Field	18
Time Zone Offset	18
Last End Field	18
NetWorker User Program Recover Option	18
Business Edition	18
Dedicated Storage Nodes Support	18
CONCLUSION	20

INTRODUCTION

LEGATO began its collaboration with Microsoft over five years ago, delivering backup solutions for the enterprise. Today that relationship continues, with solutions that protect and manage critical business data and assure the availability of applications. LEGATO will continue to embrace and extend Microsoft technologies to deliver solutions that meet changing customer needs.

The combination of LEGATO solutions and Microsoft Windows Server 2003 provides a scalable and dependable IT infrastructure that allows customers to focus on their core business with the assurance that their business-critical information is available, accessible and protected from a storage and application standpoint.

LEGATO provides unified data management solutions that ensure high-performance data protection, universal availability, and simplified management of complex storage networks. LEGATO NetWorker 7.1 introduces improved data storage and backup capabilities for the enterprise.

With LEGATO NetWorker you can quickly recover and protect massive volumes of data, increase service levels and efficiency, reduce downtime costs and administrative overhead, and lower TCO of storage resources. LEGATO NetWorker offers greater reliability, performance, and scalability of data protection operations across the enterprise.

The release of NetWorker 7.1 allows companies upgrading to Windows Server 2003 to maintain business-critical data protection. In addition to its many universal features, LEGATO NetWorker 7.1 offers a number of enhancements maximized by upgrading to Windows Server 2003, including support for the 64-bit platform, Microsoft Automated System Recovery, and Volume Shadow Copy Service. LEGATO NetWorker provides backup and recovery services for advanced Windows features such as Active Directory and safeguards the integrity of Windows system security.

LEGATO's commitment to the Windows platform is clear from its status as a Microsoft Global Gold Certified Partner for Software Products. Additionally, as a founding sponsor of the Microsoft Partner Solutions Center, LEGATO and other strategic partners are working together to design, integrate, and document innovative solutions that solve business problems in the enterprise.

With this commitment, enterprises of all sizes can be sure that their mission-critical systems and applications are supported by an operating system whose reliability, availability and security

is second to none and backed by a world-class data protection solution.

In this white paper we explore the features and benefits of LEGATO NetWorker 7.1 running on Windows Server 2003 or protecting Windows Server 2003 application servers. Many of these same features and benefits apply to the entire Microsoft Windows Server 2003 family, including Windows Storage Server 2003 for NAS solutions.

NetWorker 7.1 has passed Certified for Windows® testing at VeriTest on both Windows 2000 and Windows Server 2003. This means it has been proven to meet Microsoft's stringent reliability, availability and supportability requirements.



WINDOWS SERVER 2003 – AN OVERVIEW

Improvements across the board

The Microsoft® Windows Server 2003 operating system represents a significant advancement over the Microsoft Windows 2000 family of operating systems. Windows Server 2003 is the fastest, most reliable, most secure Windows server operating system ever offered. It features overall enhancements in reliability, availability, and manageability, as well as scalability extending to 64 processors.

The Windows Server 2003 family builds on the strengths of Windows 2000 to provide a platform that is more productive, dependable, and connected than ever before. New and improved file, print, application, Web, and communication services provide a more robust, comprehensive platform for your mission-critical business resources. Integrated features such as the Active Directory® service and enterprise-class security services allow you to provide secure yet flexible access to all the resources your users need.

FEATURES AND BENEFITS

Security

The Trustworthy Computing initiative launched by Bill Gates in January 2002 is based on four pillars: security, privacy, reliability, and business integrity. Windows Server 2003 is the first Windows operating system to ship under the Trustworthy Computing initiative.

The security innovations in Windows Server 2003 offer customers a flexible security experience, providing both a more secure out-of-the-box foundation and extensive technologies to help customers build, deploy and manage more secure solutions. Microsoft has made engineering design changes, adjusted settings to help deliver security by default, and delivered new features and technologies that enhance security for the Windows platform.

Secure by Design. Improved security of Windows Server 2003 reflects Microsoft's \$200 million investment in 2002 to reduce code vulnerabilities in its platform, modify the development process, and improve accountability at every level for security. Designed with a focus on improving security, Windows Server 2003 features a redesigned IIS, strong authentication protocols such as 802.1x and PEAP, and the common language runtime to create a safer computing environment.

-
- Internet Information Services (IIS) was redesigned in Windows Server 2003 to improve security for Web transactions. IIS 6.0 makes it possible to isolate an individual Web application into a self-contained Web service process, which prevents one application from disrupting the Web services or other Web applications on the server. IIS also provides health-monitoring capabilities to discover, recover, and prevent Web application failures. In IIS 6.0, third-party application code runs in isolated worker processes, which by default use the new lower-privileged Network Service logon account. Worker process isolation makes it possible to confine a Web site or application to its root directory through Access Control Lists (ACL).
 - Improved network communication security in addition to host security. To improve the security of wireless communication, Windows Server 2003 supports strong authentication protocols such as 802.1x (WiFi) as well as Protected Extensible Authentication Protocol (PEAP). Internet Protocol Security (IPSec), a suite of cryptography-based protection services and security protocols, has been enhanced for stronger LAN data encryption.
 - The common language runtime (CLR) software engine is a key element of Windows Server 2003 to improve reliability and help ensure a safer computing environment. CLR verifies that applications can run without error and checks security permissions to ensure that code only perform appropriate operations. CLR reduces the number of bugs and security holes caused by common programming mistakes, leaving fewer vulnerabilities for attackers to exploit.

Secure by Default. To secure Windows Server 2003 by default, the attack surface area has been reduced by creating stronger default policies (e.g., file system Access Control Lists (ACL)), redesigning IIS, and reducing the total number of services, the number of services running by default, and the number of services running as system.

- To reduce the default attack surface of Windows Server 2003, Microsoft disabled 19 services, and reduced several services to run under lower privileges. For example, in order to reduce the Web infrastructure attack surface, installing Windows Server 2003 does not install IIS 6.0 by default—administrators must explicitly select and install it. When a server is being upgraded to Windows Server 2003, IIS 6.0 will be disabled also. In addition, as IIS 6.0 is being installed, it is configured by default in a “locked down” state. After installation, IIS 6.0 accepts requests only for

static files until configured to serve dynamic content, and all time-outs and settings are set to aggressive security defaults. IIS 6.0 can also be disabled using Windows Server 2003 group policies.

- Stronger default settings are used in ACLs, which define the criteria an operating system uses to protect network resources. For example, creating the new System Root ACL and setting it as the default means that users can no longer write files to the root of the system drive, which prevents certain spoofing attacks.
- Two additional user accounts were created to run services at lower privilege levels, which helps ensure that a vulnerability in a service cannot be exploited to take over the system. The new Network Service account is used, for example, to run DNS Client and all IIS Worker Processes. Telnet now runs using the new Local Service account.

Secure in Deployment. In addition to the secure architecture design and added security features in Windows Server 2003, Microsoft offers its customers tools, prescriptive guidance, training, and services to help them deploy a secure connected infrastructure.

- Software Restriction Policy (SRP) is a new feature in Windows Server 2003 and Windows XP that gives administrators a policy-driven mechanism to identify software running in their domain and control its ability to execute. Using a software restriction policy, an administrator can confine execution to a set of trusted applications, thus preventing the operation of unwanted applications, such as viruses or software known to cause conflicts. A software restriction policy also could be used to allow only administrators to run certain programs on shared machines.
- Security Configuration Editor (SCE) is designed to help businesses secure Windows systems operating in various roles and deployment scenarios, such as a Web server that is connected both to the Internet and to a secure internal network. The goal of SCE is to help customers maximize the security of such systems without sacrificing their required functionality. For example, services (e.g. Fax) that may not be required for file server role can be disabled. Administrators can use the Security Configuration Wizard in SCE to construct security policies for their different types of servers, and perform Lockdown Testing to verify that systems function as expected. This tool will be released in the later part of 2003.

-
- Microsoft Audit Collection Services (MACS) is a tool to monitor and audit systems. MACS collects security events in a compressed, signed, encrypted manner and loads the events into a SQL database for analysis. This tool works with Windows XP, Windows 2000 Server, and Windows Server 2003, and uses existing security technologies to protect against tampering and disclosure during network transit. It enables the separation of auditor and administrator roles to ensure that administrators cannot make changes to audit information. This tool will be released in the later part of 2003.

Internet Information Services 6.0

One of the key security enhancements in Windows Server 2003 is the complete redesign of Internet Information Services (IIS). Internet Information Services 6.0 is a powerful Web server available in all versions of Windows Server 2003 that provides a highly reliable, manageable, scalable, and secure Web application infrastructure.

IIS 6.0 makes it possible for organizations of all sizes to quickly and easily deploy powerful Web sites and applications, and provides a high-performance platform for all applications. Applications built with Microsoft .NET frameworks are faster and more reliable on IIS 6.0 due to the integration of the .NET frameworks into the IIS 6.0 process model. IIS 6.0 features a new fault-tolerant process architecture with health monitoring that runs all application code in an isolated environment for maximum reliability and availability.

Web server administration is simplified using an XML-based configuration file that can be modified without having to stop and restart the server. IIS 6.0 enhancements such as kernel-mode caching and "Web gardens" dramatically increase the product's scalability and performance compared to previous versions of IIS. In terms of security, IIS 6.0 is not installed by default with Windows Server 2003 and is fully "locked down" when first installed to reduce attack surface area. The benefits of choosing IIS 6.0 include less planned and unplanned system downtime, increased Web site and application availability, lower system administration costs, server consolidation (reduced staffing, hardware, and site management costs), and a significant increase in Web infrastructure security.

Scalability

Windows Server 2003 takes the scalability gains on Windows 2000 Server Family to a new height. Windows Server 2003 is designed for both scale-up and scale-out scenarios. Scale-up scenarios are enabled by symmetric multiprocessing (SMP) and CC-NUMA (Cache Coherent Non-Uniform Memory Access)

optimizations, and scale-out by the various types of clustering provided by Microsoft.

Windows Server 2003 scales from single processor solutions all the way up to 64 processors in a single partition and offers 8-node clustering with Enterprise and Datacenter Editions. In comparison, Windows 2000 Server scaled to 32 processors and offered up to 4-node clustering.

Internal tests indicate that, compared to Windows 2000 Server, Windows Server 2003 delivers up to 140 percent better performance in the file system and significantly better performance in various other features, including Microsoft Active Directory service, Web server, Terminal Server components, and networking services. Key scalability enhancements include:

- **64-Bit Support.** Windows Server 2003 offers support for 64-bit architecture with Enterprise and Datacenter Editions. With 64-bit architecture, Windows offers scalability up to 64 processors and 512 GB of RAM. Customers can get even more performance and scalability in high-end database and LOB (line of business) application scenarios that demand the utmost for memory-intensive or computational-intensive tasks.
- **Support for Intel Hyper-Threading.** Intel Hyper-Threading Technology (HT) allows a single physical processor to execute multiple threads (instruction streams) simultaneously, potentially providing greater throughput and improved performance. In general, multithreaded Windows applications perform better when running unmodified on an HT processor than they do on a similarly equipped single-threaded processor. Windows Server 2003 32-bit platforms provide HT support both on architectural and licensing fronts.
- **NUMA Optimization.** Windows Server 2003 provides enhanced NUMA (Non-Uniform Memory Access) support. Most Windows applications will perform optimally without modification on NUMA systems running Windows Server 2003 due to the automated NUMA features in the operating system. NUMA support is offered only on 32-bit and 64-bit Enterprise and Datacenter Editions.
- **Hot Add Memory.** This new feature allows ranges of memory to be added to a compatible computer and made available to the operating system and applications as a part of the normal memory pool. This does not require rebooting the computer or other

downtime. Hot Add Memory is offered only on 32-bit versions of Enterprise and Datacenter Editions.

Reliability and Availability

Reliability and availability are woven into every aspect of Windows Server 2003 design to provide better customer experience. Key highlights include:

- **8-Node Clustering.** Windows Server 2003 supports 8-node clustering with 32-bit and 64-bit Enterprise and Datacenter Editions. This is an increase from 2- and 4-node support in Windows 2000 Advanced and Datacenter Servers respectively. 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. The addition of 8-node clustering offers increased deployment flexibility, particularly for geographically dispersed cluster configurations.
- **Majority Node Set.** 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 such as server clusters with no shared disks can be built. Majority Node Set also makes it easier to build and configure multi-site, geographically dispersed clusters.
- **Network Load Balancing Manager.** This new utility in Windows Server 2003 provides a single point of configuration and management for NLB clusters. NLB Manager can be used to create new NLB clusters and automatically propagate cluster parameters and port rules to all hosts in the cluster, add and remove hosts to and from NLB clusters, automatically add Virtual IP (VIP) addresses to TCP/IP, manage existing clusters by connecting to them or by loading their host information to a file and saving this information for later use, configure NLB to load balance multiple Web sites or applications on the same NLB cluster, and diagnose improperly configured clusters.
- **Datacenter High Availability Program.** The Datacenter Program has been expanded to meet the growing customer demand for higher availability on Windows. The new Datacenter High Availability Program strengthens the support and services model, expands the range of support providers, and merges the Joint Support Queue (JSQ) with the new Microsoft

High Availability Resolution Queue (HARQ). The improvements to the support and services model enable vendors to act in a unified, consistent way. This new model ensures our mutual customers they can achieve the highest levels of reliability and availability from the Datacenter Server platform. In addition, the Datacenter High Availability Support Program has added change management and configuration auditing services as required practices to participate in the program.

- **Storage Area Networks.** Storage Area Networks (SANs) are significantly easier to use in Windows Server 2003. Administrators can control volume mounting with the aid of a SAN-friendly configuration, 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 a SAN is greatly enhanced in Windows Server 2003.
- **Memory Mirroring.** Memory mirroring provides the ability to take snapshots of independent memory sub-systems in a Fault Tolerant set of computer systems so they can have the same replicated memory.

Manageability

Management capabilities delivered with Windows Server 2003 are designed to simplify and automate the management of Windows environments while providing the flexibility and reliability necessary to meet the business needs of customers. Windows Server 2003 includes new and enhanced management capabilities to address the challenges faced by customers and improve the manageability of Windows Server environments. Key highlights include:

- **Active Directory Enhancements.** Active Directory in Windows Server 2003 provides customers increased flexibility and manageability. Examples of the enhancements include secure credential and certificate management to provide a consistent single sign-on experience; health monitoring visibility to easily monitor trusts and replication activity; improved interfaces (e.g., multi-select and bulk-edit users, Resultant Set of Policy [RsoP], Group Policy Management Console [GPMC], new setup wizards and DNS "self-diagnostics"); domain rename to allow customers to easily rename one or more already deployed domains and create a different domain-tree structure; design flexibility via Cross-Forest Trust, enabling autonomy with interoperable authentication and the ability to share files and other resources

across forests; schema enhancements to easily redefine attributes or class definitions and deactivate unused or no longer needed elements without rebuilding the Global Catalog.

- **Policy Based Management.** Policy-based management provides fine-grained control over the definition and enforcement of IT policies. Policy-based management enables 'one-to-many' management, making it almost as easy to manage very large distributed systems environments as to manage a single system or user, once the policies have been defined. Windows Server 2003 unleashes the power of policy-based management via improved Group Policy infrastructure, new and vastly improved Group Policy management capabilities, and broad support for policy-based management across server components.
- **Automated Deployment.** Windows Server 2003 includes new and enhanced capabilities to automate the deployment and redeployment of the operating system and applications. Remote Installation Services (RIS) enables fully automated script-based or image-based deployments to servers and desktops. In conjunction with Windows PE, the new Windows pre-installation operating system environment, RIS enables complete automation of highly customized deployments. The new Automated Deployment Services (ADS) includes a new set of imaging tools developed by Microsoft and a secure, remote-able infrastructure for rapidly deploying and re-deploying servers in high-bandwidth data center environments. In addition, ADS offers a secure, reliable script execution framework that lets administrators perform script-based administration on 1,000 servers as easily as they once did on a single server.
- **Effective User Service Management.** IntelliMirror® – the ability to provide users with consistent access to their applications, roaming user profiles, and user data from any managed computer – even when they are disconnected from the network, is enabled by Windows Server 2003 technologies such as Active Directory, Group Policy, Software Installation, Windows Installer, Folder Redirection, Offline Folders, and Roaming User Profiles. This also enables centralized backup of user data and configuration files by the IT organization. As part of Volume Shadow Copy service, this feature lets administrators configure point-in-time copies of critical data volumes without interrupting service. These copies can then be used for service restoration or archival purposes. Together, these capabilities result in high levels of user productivity, satisfaction, and

data safety.

- **Enhanced Security Management.** Windows Server 2003 provides powerful capabilities to establish and manage the security of your Windows environment. The ability to restrict and delegate rights for specific administration roles, software restriction policy enforcement, strong password requirement enforcement, and the ability to deliver highly managed user environments minimizes the risk of unintentional or deliberate security breaches. Also included is Software Update Services (SUS), a solution that enables automated download of security & critical operating system updates and gives administrators control over the testing, staging, distribution, and application of these updates within their organizations.
- **Scalable Operations Management.** Remote administration is enabled via Terminal Server, Windows Script Host and Windows Management Instrumentation (WMI), the management infrastructure that provides access to over 10,000 system objects in Windows Server 2003 via application, scripting, and command line interfaces. WMI allows fine-grained discovery, monitoring, control, and reporting of system and application settings and state. Windows Server 2003 also includes built-in performance monitoring, logging, tracing, and system recovery capabilities to enable quick troubleshooting and resolution of abnormal operating conditions. With the Microsoft Services for UNIX 3.0 product (a separately licensed add-on), Windows Server 2003 delivers a complete UNIX environment on Windows and allows IT organizations to leverage their investments in UNIX scripts and expertise to do unified management of Windows and UNIX environments.
- **Windows System Resource Manager (WSRM).** WSRM enhances application availability and quality of service by providing control over application CPU and memory utilization, making it easier to run mixed application workloads on a single server. You can use WSRM to manage multiple applications on a single computer, users on a remote computer (with Terminal Services installed), IIS app pools, or virtual machines. Managing resources with WSRM improves system performance and reduces the chance that applications, services, or processes will interfere with the rest of the system. This aligning of IT resources with business priorities creates a more consistent and predictable experience for users of applications and services running on the computer. WSRM's accounting tracks resource usage, which results in improved

understanding of application resource utilization; this accounting data can serve as the basis for charge backs and capacity planning. WSRM is offered on 32-bit and 64-bit versions of Windows Server 2003, Enterprise and Datacenter Editions.

LEGATO NETWORKER 7.1

"The new innovative storage features in Windows Server 2003 will extend LEGATO's capabilities to deliver cost-efficient, reliable and scalable storage solutions to its customers."

Charles Stevens
Corporate Vice President of Sales and Marketing
Microsoft Enterprise Storage Division

Version 7.1 of NetWorker includes new features that take advantage of Windows Server 2003 to provide backup and recovery scenarios that are robust, scalable, and flexible. Coupled with centralized management, structured metadata, and Open Tape Format, NetWorker specifically addresses and facilitates fast data backup and recovery.

Removable Storage Support

NetWorker 7.1 supports the Microsoft Removable Storage feature of Windows Server 2003. No additional Microsoft or LEGATO software is required to use Removable Storage with NetWorker software. The Microsoft Removable Storage service acts as an agent to the NetWorker server or storage node software to perform the actual mounting, labeling, and tracking of media. Removable Storage controls the data storage hardware's doors, drives, and robotics, and performs uniform drive cleaning operations. NetWorker performs volume and file management, which is not provided by the Removable Storage service.

Use of Removable Storage is optional with NetWorker software. You may prefer to disable Removable Storage in some cases, such as when you want NetWorker software to have exclusive use of a storage library. A primary advantage in using Removable Storage is that it allows multiple data management applications to share access to the same storage hardware.

Volume Shadow Copy Service Support

LEGATO NetWorker 7.1 uses the Windows Server 2003 Volume Shadow Copy Service (VSS) to provide backup functionality for active applications and services. VSS coordinates between applications, NetWorker, and the storage sub-system to ensure that the point-in-time copies (snapshots) of volumes/data is consistent as defined by the applications. Production applications will implement a very brief "freeze/thaw" semantic

with minimal or no impact on end users while VSS and NetWorker take a copy of the data volume(s).

NetWorker DiskBackup

Release 7.1 of the NetWorker software offers two ways to save data to a computer's local or network-attached disk:

- File Type Device
- Advanced File Type Device (Adv_file)

Storing data using the NetWorker DiskBackup solution greatly reduces the time it takes to both save and recover data compared to using tape. The Advanced DiskBackup™ Option allows simultaneous reads and writes, lets you protect multiple clients in parallel, and automatically removes bad and/or expired backups.

Automated System Recovery Support

Microsoft Automated System Recovery (ASR) is a standard feature of Windows Server 2003. No additional Microsoft or LEGATO software is required to use ASR with NetWorker software.

ASR enables NetWorker to implement an automated method of fully recovering a failed host computer. NetWorker software supports ASR save set backup and recovery, and ASR disaster recovery on a NetWorker client only.

The NetWorker ASR save set contains the files necessary for Windows to perform an ASR Disaster Recovery if the system disk should stop functioning. ASR also contains the information necessary to gain access to the appropriate backup files and run NetWorker recovery automatically.

NetWorker ASR support allows you to create a boot diskette for recovery, and requires the Windows 2003 distribution media (CD) of the system be available during recovery. For more information, see the Windows Admin guide (winag.pdf).

Cluster Awareness

LEGATO NetWorker 7.1 provides data protection for highly available applications configured using the improved scalability features in Microsoft Cluster Services (MSCS) introduced with Windows Server 2003. The NetWorker server can run in an MSCS environment as either a stand-alone or a highly available application. NetWorker Server 7.1 can also be a highly available application when configured as a cluster resource within an MSCS environment.

If the NetWorker server is configured as a cluster resource, and a scheduled backup or save is interrupted due to failure of the node that hosted the NetWorker software, the NetWorker server fails over to another node. This allows the interrupted backup to continue with minimal disruption.

64-bit Version Support

In addition to its 32-bit offering, a 64-bit version of LEGATO NetWorker is available in order to fully protect Windows Server 2003 running on Intel 64-bit architecture.

TapeAlert Capability

The new TapeAlert feature displays diagnostic and status messages for devices. These messages may give:

- Critical diagnostic information, such as for media or drive failure, when user intervention is urgent and data is at risk.
- Warnings when the media or device needs servicing.
- Information regarding media or device status.

Unique Identification of Devices

The current NetWorker release contains the following enhancements to make device configuration easier:

- The *inquire* command has been enhanced to uniquely identify attached devices by a combination of identifiers, including manufacturer, product ID, serial number, World Wide Number (WWN) and World Wide Port Name (WWPN).
- A new command displays the attached devices in the order of their element connection.

The output of these commands may be useful when configuring autochanger(s) that contain many drives by reducing guesswork or manual inspection when determining drive order.

Service Mode for Devices

This release permits devices to be put into a "service" state. Devices in this state are removed from automated allocation, but they are able to complete their current or pending backup and recovery operations.

Improved Error Handling for Lost Volume Names

The NetWorker software has improved error handling and reporting to the media database that ensures an inventory is correctly updated after an unsuccessful read label operation.

This enhancement allows the NetWorker software to update an autochanger resource and avoid an infinite loop of subsequent unsuccessful mounts for the same volume.

User Group Resource

The NetWorker software includes an access control feature that is configured through a new User Group resource, allowing NetWorker administrators to assign users to one of two pre-configured NetWorker user groups:

- **Administrators.** Members of the Administrators group have permission to perform all NetWorker functionality. Members of the Microsoft Windows Administrators group are always assigned to this group and cannot be removed from the group.
Note: Privileges associated with the Administrators group cannot be changed.
- **Users.** By default, members of the Users group are granted permission to back up and recover local data and to monitor NetWorker operations, but cannot view or edit configurations. You can change the privileges associated with the Users group by adding or removing privileges.

You can add new users to either the Administrators or Users groups, and you can edit the privileges associated with the Users group. However, you cannot create or delete NetWorker user groups.

Monitoring NetWorker Resources

The Monitor Resource Allocation Protocol (RAP) option tracks the history of additions, deletions, or modifications to a NetWorker resource or resource attribute and records those changes in a log file. The log file lists the user name, the source computer, and the time of the modification. You must have Administrator privilege to enable this feature.

Note: By default, the Monitor RAP option is disabled.

Generating Program-Readable Reports

The NetWorker software lets you generate reports in formats that scripts and computer programs can easily parse. Two formats are available for output:

- Delimiter-separated values format
- XML format

Comment Attribute in NetWorker Resources

A Comment attribute has been added to each NetWorker resource, allowing NetWorker administrators to provide unique descriptions of each resource instance. For example, if there are multiple Client resources with the same name, the Comment attribute can be used to distinguish each resource.

User Identification Field

An attribute named *User ID* has been added to the NetWorker Administrator program. This read-only field identifies the user that is currently using the NetWorker Administrator Program.

Time Zone Offset

To enable management and reporting applications to properly handle NetWorker servers in different timezones, the server's local time is displayed as an offset from GMT. This value is displayed in the Server window of the NetWorker Administration Program.

Last End Field

The Last End field is an information-only field that displays the time at which the last save group completed. The Last End field is updated if the Last Start field is updated and the save group completes normally. A save group will not complete normally if there is an abnormal shutdown such as a computer crash or core dump.

NetWorker User Program Recover Option

The Recover option under the Operation menu browses and recovers indexes and data for remote clients. This new functionality merges the Recover and Directed Recover functionality.

Business Edition

A new level of the NetWorker server is available: Business Edition. NetWorker Business Edition is the same as the existing Workgroup Edition, with the addition of a license to use an autochanger (1-26 slots) as part of its base enabler, the ability to back up a two-node cluster client, and support for NDMP connections.

Dedicated Storage Nodes Support

A dedicated storage node takes the place of a SAN storage node in this release of NetWorker. All devices in NetWorker version 7.1 and later created on storage nodes (with the exception of servers) include the Dedicated Storage Node

attribute. A dedicated storage node can only back up its own local data.

This attribute is set at the time a device is created on a remote storage node. If the Dedicated Storage Node attribute is set to Yes, you will need a Dedicated Storage Node License for the storage node. If the Dedicated Storage Node is set to No (the default value), a standard storage node license is required. All storage nodes prior to NetWorker version 7.1 will behave as if the Dedicated Storage Node attribute is set to the default No.

CONCLUSION

LEGATO NetWorker 7.1 ensures that environments migrating to Windows Server 2003 will maintain complete data protection and storage integrity. NetWorker offers superior universal backup and recovery functionality, and has been enhanced to take advantage of Windows Server 2003 innovations.

Enterprises utilizing Windows Server 2003 and LEGATO NetWorker 7.1 will enjoy a consistent, reliable and fully protected IT architecture that is flexible enough to accommodate and exploit future challenges.

Above all, customers can be certain that there is a long-term commitment by both Microsoft and LEGATO to support and leverage future developments of their respective technologies. LEGATO's support of the Windows platform along with its adoption of other Microsoft supported initiatives demonstrates the extent of this collaboration as well as the determination of both organizations to offer the best enterprise-wide solutions to the marketplace

Microsoft, Windows, Windows NT, BackOffice, SQL Server, Windows 2000 and Windows Server 2003 are registered trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are held by their respective companies.

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, in this summary.

© 2003 Microsoft Corporation and LEGATO Systems, Inc. All rights reserved.

