

# The White Papers

## **Plan, Deploy and Manage Windows 2000**

Technical Brief

**Quest Software**

## Contents

---

<b>Introduction.....</b>	<b>3</b>
<i>Overview: Windows NT/2000 Domain Management.....</i>	3
The Microsoft Directory Service Strategy.....	4
The Benefits of Active Directory .....	5
About Security Identifiers (SIDs).....	6
The Windows 2000 Business Case.....	7
<b>The FastLane Lifecycle .....</b>	<b>8</b>
<i>Planning.....</i>	8
Key Planning Points: .....	9
The Quest Software Approach .....	9
<i>Consolidation.....</i>	11
Key Consolidation Points:.....	11
The Quest Software Approach .....	12
<i>Migration .....</i>	13
Key Migration Points: .....	13
The Quest Software Approach: .....	14
<i>Clean-Up.....</i>	15
Key Clean-Up Points.....	15
The Quest Software Approach .....	16
<i>Administration.....</i>	17
Key Administration Points .....	17
The Quest Software Approach .....	17
<b>Summary .....</b>	<b>18</b>
<b>About Quest Software.....</b>	<b>19</b>
<b>Glossary .....</b>	<b>20</b>

# Plan, Deploy and Manage Windows 2000

By Quest Software

## Introduction

Quest Software has persistently provided scalable, enterprise-wide tools that not only solve real-world challenges, but also enhance the performance of IT resources, and consequently, offer an improved return on investment.

The introduction of new enterprise technology occasions both opportunity and concern: network professionals must cross uncharted territory in order to achieve the anticipated benefits. With extensive capabilities in Directory Management, coupled with a network of strategic global partners and distributors, the FastLane Suite™ of solutions is ideally positioned to complement and extend the value propositions of Microsoft® Windows® 2000 and Active Directory™ (AD).

This paper explores Windows NT®/2000 domain management, Active Directory, and the Windows 2000 business case – with the intent of highlighting the compelling rationale for large enterprises, considering a Windows 2000 implementation, to adopt the FastLane methodology as effective in lowering the total cost of ownership.

Quest Software maintains, as shall be demonstrated in this document, that many significant Windows 2000 benefits are predicated on AD being fully and properly deployed.

## Overview: Windows NT/2000 Domain Management

Microsoft Windows NT and its successor, Windows 2000, have fundamentally different approaches to managing resources and users. Active Directory, the directory service integrated with Windows 2000 Server, allows the organization of resources and users into a unified logical structure – a feature not present in NT.

However, similar to Windows NT, the administrative foundation of Windows 2000 is the domain – that is, all network objects exist within a domain.

Further, domains are units of replication. A single domain may span multiple physical locations or sites. Unlike the single-master model used by Windows NT 3.X and 4.0, with its Primary Domain Controllers and Backup Domain Controllers, AD uses a multi-master “peer controller” model. Therefore, all the domain controllers that govern a given domain can receive changes directly and propagate those changes.

Multiple domains within AD are linked to a domain tree - a hierarchical structure of domains that form a contiguous namespace (a collection of domains with a common DNS root name)

Operating Systems in use as reported by IT professionals  
(Source: International Data Corp.)

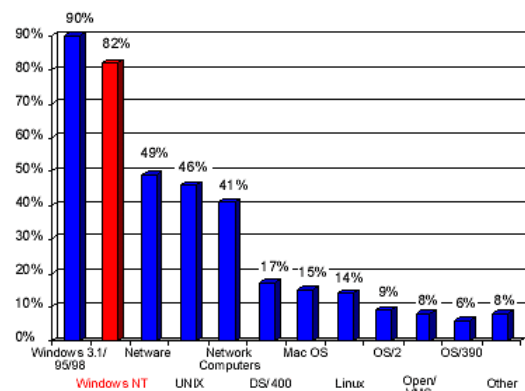


Figure 1: Windows NT market space dominance

and share a common schema, configuration and global catalog. Users in the linked domains can access resources in other domains via transitive trust relationships that are structured hierarchically among all of the domains in the domain tree.

A forest is a group of one or more trees connected by Kerberos trusts, organized as peers. This provides organizations with the option of constructing their enterprises from separate, distinct, and disjointed namespaces.

Organizational units (OUs), containers that hold objects such as users, groups and printers in AD, can be created within domains. In turn, OUs may be organized into a logical structure that corresponds to specific corporate requirements. Early versions of Windows NT could support only 10,000 objects (such as Windows NT user IDs, groups, and workstation accounts). Organizations with more than 10,000 users or Windows NT workstations had to divide their network into multiple Windows NT domains. AD can maintain at least 10 million objects (resources) - network users, groups and computers - in a single domain.

### The Microsoft Directory Service Strategy<sup>1</sup>

Many vendors build specialized repositories or directory services into their applications and devices to enable the specific functionality their customers require. For example, e-mail products include directory services that let users look up and send mail to others. And server operating systems use directory services for features such as user account management and storing configuration information about applications. Because these directory services are targeted narrowly to the needs of the application or device and often lack standards-based interfaces, most companies have found that they are responsible for many different directories that cannot be managed centrally or interoperate easily with each other. Having many incompatible directory services means that:

- End users must use multiple user accounts and passwords to log in to different systems, and they must know the exact locations of information on the network
- Administrators must understand how to manage each directory within the network and must duplicate many steps whenever procedures, such as adding or removing a new employee to a company, involve many different directories
- Application developers must write different logic for every directory that their applications need to access

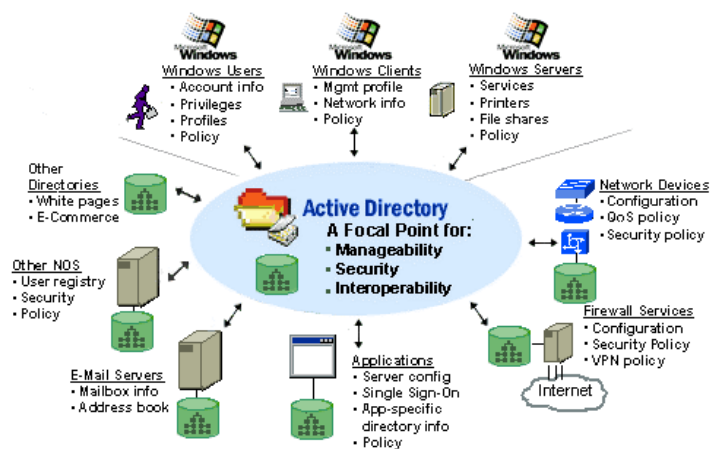


Figure 2: AD is a consolidation point for many of the existing application-specific directories. Copyright © 2000, Microsoft Corp.

The proliferation of customized directory services translates directly into a continually rising cost of ownership: it requires greater management, necessitates applications that are more complex and adversely affects the productivity of the end user. Companies can halt this trend and minimize the total number of directories that they have through proactive directory

<sup>1</sup> Based on 'Planning for a Global Directory Service'. Microsoft Corp. March 1999.

consolidation. The best solution is to standardize based on technologies that provide the required levels of scalability, standards-based interoperability and operating system integration.

## The Benefits of Active Directory<sup>2</sup>

Microsoft defines AD as “an essential and inseparable part of the Windows 2000 network architecture that improves on the domain architecture of the Windows NT 4 operating system to provide a directory service designed for distributed networking environments.”

Active Directory is an enterprise-class directory service that is scalable, built using Internet-standard technologies, and fully integrated with the operating system. In addition to providing comprehensive directory services to Windows 2000, AD is designed to be a consolidation point for many of the existing application-specific directories that exist today. This makes AD a foundation for corporate information sharing and common management of network resources, including applications, network operating systems, and directory-enabled devices.

AD brings together standards-based technologies such as Lightweight Directory Access Protocol (LDAP), Directory-Enabled Networks (DEN), Kerberos and Hypertext Transfer Protocol (HTTP).

Importantly, AD centralizes all of the user, group, application, device, printer and computer information on a network in one central repository.

Totally integrated with Windows 2000 Server, Active Directory:

### Simplifies management tasks:

- Eliminates redundant management tasks with a single-point of management for Windows user accounts, clients, servers, and applications as well as the ability to synchronize with existing directories
- Reduces trips to the desktop. Automatically distributes software to users based on their role in the company, reducing or eliminating multiple trips that system administrators need to make for software installation and configuration
- Better maximizes IT resources. Securely delegates administrative functions to all levels of an organization

### Strengthens network security:

- Improves password security and management. By providing single sign-on to network resources with integrated, high-powered security services that are transparent to end-users
- Ensures desktop functionality. By locking-down desktop configurations and preventing access to specific client machine operations, such as software installation or registry editing, based on the role of the end-user
- It speeds e-business deployment by providing built-in support for secure Internet-standard protocols and authentication mechanisms.

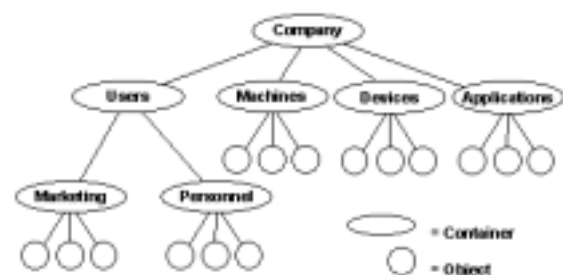


Figure 3: AD organizes information hierarchically to ease network use and management.

<sup>2</sup> Based on 'Active Directory Overview'. Microsoft Corp. June 30, 1999.

**Extends Interoperability:**

- Takes advantage of existing investments to ensure flexibility. Standards-based interfaces to all features make use of investments and ensure flexibility for future applications and infrastructure. Consolidates management of multiple application directories. Using interfaces, connectors, and synchronization mechanisms, organizations can consolidate directories including Novell's NDS, LDAP, ERP, e-mail, and other applications
- Allows organizations to deploy directory-enabled networking. Network devices from vendors such as Cisco and 3COM can use the directory to let administrators assign quality of service and allocate network bandwidth to users based on their role in the company
- Allows organizations to develop and deploy directory-enabled applications. Using the fully extensible directory architecture, developers can build applications that deliver functionality tailored to the needs of the end user

**Provides policy-based administration:**

Group Policies are configuration settings applied to computers or users as they are initialized. All Group Policy settings are contained in Group Policy Objects (GPOs) applied to AD sites, domains or organizational units. GPO settings determine access to directory objects and domain resources, what domain resources (such as applications) are available to users, and how these domain resources are configured for use.

**About Security Identifiers (SIDs)**

Domain reconfiguration is intricate because it requires that the network administrator update existing resources within the network. In other words, if John currently has access to a desktop computer, files on a server, and his email, he will want to have the same access to information after the migration. Ideally, he will not notice that the migration has occurred. What makes this changeover so difficult is the fact that John is only granted access if his **SID (Security Identifier)** is recognized by the resource he wishes to access.

Because SIDs are domain-specific, if the company eliminates John's domain, his access to resources must be replicated in the new domain. It would be impractical to attempt this task manually, particularly for a large number of users, because the job entails searching for John's SID in all of the access control lists, groups, user rights, Windows NT profiles and network applications in the original domain and other domains. *An application that automates this process is therefore necessary.*

*Consider this analogy:* Imagine that your office is located in the east end of a large commercial building. The large room adjacent to your office houses your critical files, personal information and your telephone, and you can access this room by means of a door key. You are relocated to the west end of the building, and your new office is also adjacent to the same central resource room. Your old key is taken away and you are issued a new key. Therefore, your key does not unlock the door and so you cannot access your telephone and files. The locks must be changed to accommodate a new key.

This is what happens when the user's new SID no longer enables access to resources as a result of a domain consolidation, except the latter case is far more complex because of the difficulty in finding all of the access points (or locks) within the enterprise. The migration's success depends upon the administrator's ability to locate and append the user's new SID to all of the resources that exist in the network, including files, shares, computers, and groups.

Windows 2000 introduces the concept of the SIDHistory. Under rigid and controlled conditions, this feature allows a user account to be migrated to a new domain and maintain access to the same resources that could be accessed by the source account. To further our analogy, the office's Security Department must now track who has keys to which locks, thereby making the enforcement very challenging on an on-going basis.

It should be noted that SIDHistory will only work between different AD forests or when migrating from a Windows NT 4 domain to an AD domain. Migration between AD domains within a forest requires the exact same process as a Windows NT 4 migration.

## The Windows 2000 Business Case

Arthur Andersen, in the report, *Microsoft Windows 2000 Server: ROI Impact for Corporate Customers*, (August, 1999), summarizes the benefits that enterprises can expect by deploying Windows 2000:

- *Enhanced Distributed Services* – including AD directory services, standards-based security, management tools (like IntelliMirror) which allow the organization to create policy and perform more centralized management and oversight of a distributed environment
- *Enhanced Reliability and Availability*– through many system enhancements including the Distributed File System, Enhanced Clustering Services and a reduction in the number of scenarios which require system reboots or service restarts, to ensure greater system uptime
- *Enhanced Scalability* through improved Symmetric Multi-Processing, Network Load Balancing and EMA (Enterprise Memory Architecture)
- *Enhanced application support*, through the integration of a number of services into the COM+ component model enabling integrated web-based applications
- *Enhanced interoperability* through adherence to standards including X.500 style hierarchical naming structure for directory information, and LDAP for access to and from the directory, and other industry standards allows the organization greater ease of communicating within heterogeneous environments

In conclusion, the study determines that:

- Windows 2000 can have a significant positive impact on overall cost and control of IT assets
- Windows 2000 appears to be more scalable, reliable and manageable than Windows NT Server 4.0 with Service Pack 5
- Windows 2000 has enough new features to have a learning curve, or front-end training requirement, which some organizations will find significant, and against which a future stream of cost savings and benefits should be weighed
- Greater value will be more readily apparent to the larger enterprise, especially one that is already committed to a Windows NT Server 4.0-based environment
- When implemented properly, the ability to organize the IT infrastructure in a manner similar to the business organization will potentially improve' manageability and information availability
- In today's fast changing business environment, taking early advantage of the potential of Windows 2000 could positively impact the bottom line of an organization

As Microsoft states, AD is an "inseparable part of the Windows 2000 network architecture." Windows 2000 Magazine furthers this claim with the assertion, "If the migration to Active Directory can be achieved... then it will be far easier to reap the other benefits of Windows 2000, such as better reliability, scalability, security and systems management." ('IT Agenda 2000', January, 2000).

*Therefore, a properly deployed AD will assist organizations in achieving the benefits of Windows 2000, including increased scalability, manageability, and higher availability.*

## The FastLane Lifecycle

The popularity of the FastLane lifecycle for Windows 2000 deployment is based on the core need of large enterprises for a structured, tested, simplified and supported approach toward deploying the new operating system. As PC Week Magazine suggests, “The problem, for now, is getting [to Windows 2000]. Our testing showed that moving a large organization from NT4 domains to Active Directory requires extensive planning...”

This paper has devoted attention to discussing the benefits of both Windows 2000 and AD: empirical data from early enterprise adopters further corroborates Windows 2000 value proposition. The compelling rationale for Windows 2000 in turn leads to a consideration of the optimum methodology necessary to achieve a significant return on investment. Such considerations contributed to the development of the FastLane process for Windows 2000 deployment.

The FastLane lifecycle is a five-step, holistic approach to deploying Windows 2000 quickly, efficiently, while minimizing risk.



## Planning

### Key Considerations:

- What is your Windows NT/2000 co-existence strategy?
- Have you identified the source(s) of directory data for AD?
- When are you planning to migrate to Windows 2000?
- Have you developed a budget for migrating to Windows 2000?
- Do you have the internal expertise to migrate to Windows 2000?
- Have you completed your namespace planning?
- Will your AD structure be based on business units, cost centers, geographic boundaries, etc.?
- Have you designed your AD site topology?



Stuart Kwan, Program Manager, Windows NT Distributed Systems, Microsoft, comments,

*“One of the first key things you have to do when deploying Windows 2000 is design an Active Directory structure... Windows 2000 deployment planning for Active Directory involves three steps: assessing your current environment, doing structure planning, and then doing migration planning.*

*“Remember, it’s an iterative process. After you’ve done your migration plan, go back to your structure plan and see if there are any kinds of efficiencies that you can realize. The plan that you’re going to start with is structure planning and structure planning is going to*

*involve a forest plan, a domain plan for each forest, an OU plan for each domain, and a site plan for each forest. While you're doing your planning, remember to keep the guiding principles in mind. Keep it simple and anticipate any kind of change you may have in your environment."*

### Key Planning Points:

- Most Windows NT 4 domain structures typically contain objects that are invalid or unassigned, not configured properly or not appropriate for a Windows 2000 upgrade
- Enterprises are moving to a hierarchical administrative structure in AD yet have no way to model or test this in order to train people on their new roles and responsibilities
- Windows NT user and group databases are notorious for being full of dirty data; this has been allowed to continue because of the lack of resources to deal with the problem
- The migration to AD is a great opportunity to cleanse the existing user/group database of Windows NT 4, which will ensure that security risks are minimized and the licensing cost for new software that is dependant on the number of objects under management in AD is minimized
- Windows 2000 servers may have a very different role in a Windows 2000/AD environment. An upgraded NT 4 file and print server may be a domain controller, Exchange server, SQL Server or a web server in the new environment. In place upgrades of these machines will bring all the security setting that were in place on NT 4. Tighten security now in order not to have exposed servers in Windows 2000.

"Your migration goals might be business-related or relate to the migration itself.

"Business-related goals in most cases will drive the initial migration decision. This type of goal involves making implementation choices, and can be used to evaluate possible trade-offs... Migration-related goals involve the results of the migration, and might be influenced by concerns such as disruption to production systems, final system performance, and mean time between failures. These goals can determine how test plans and acceptance criteria are formulated."

*-Planning Migration from Windows NT to Windows 2000, Microsoft Corp., 1999*

### The Quest Software Approach

- Assess current NT & Exchange environment
- Establish policy-based exception reporting
- Cleanse the NT4 user & group database
- Find computers that will not upgrade
- Eliminate Security holes that could be migrated
- Assess the mailbox data in Exchange 5.5

A significant issue during the planning process is ascertaining which parts of the existing infrastructure will support the migration to Windows 2000. Administrators must know the status of their existing NT 3.51/4 environment in order to install whatever Service Packs may be required to ensure a level migration field.

The capacity inventory will invariably produce surprises. For instance, many companies have installed their Windows NT 4 Server on a half-gigabyte primary partition. Unfortunately, this typical partition size does not accommodate Windows 2000, so organizations need to evaluate disks, processor speeds and RAM on all NT 4 servers to ensure they have the required hardware for the upgrade.

Assessing the network presents an ideal opportunity for determining the extent of redundant information in the environment. 'Garbage data' can impede a migration project by invalidating

new corporate standards. To avoid this scenario, managers need to gather timely, accurate information on local group memberships, local user lists, local groups by computer, which users have administrator status - and ensure that only this up-to-date information is migrated to the new system. Security holes, such as inactive accounts, shares with 'Everyone Full Control', domains with AUTOLOGON and NULL passwords, must also be identified lest they open up security holes: achieving full status reports of these helps to gather crucial exceptions that would otherwise override defined policies.

One of the largest and most important planning considerations—and one that will be new to many NT administrators—involves decisions about namespace design, the AD hierarchy, OUs and delegation of administrative rights. Once in place, these cannot be changed without significant effort. Having a method to model a new namespace before rollout can add value and reduce risk to the new system, allowing managers to get validation and acceptance from all the stakeholders before the structure is implemented.

During the Planning/Assessment step, the FastLane Suite enables an enterprise to:

1. Create administrative structures that match the business requirements of an organization - which can be tested and refined on NT4 before the actual migration to AD. These structures may be maintained before, during and after migration, which in turn shelters end users and the help desk from the disruptions.
2. Access comprehensive reporting and assessment capabilities, including:
  - Searching for invalid accounts, preserving the cleanliness of the new environment, and decreasing software licensing costs
  - Identifying hardware that will not support a Windows 2000 upgrade
  - Determining budget requirements for Windows 2000 upgrade and planning the roll-out by assessing hardware update needs
  - Searching for security violations in the current structure

Windows NT Administrators are challenged on a daily basis to understand the overall state of the directory objects in Windows NT and Microsoft Exchange. The FastLane Suite provides a unified view of the network and its policies that typically include multiple domains and Microsoft Exchange servers. An administrator can select any domain and object or container within that domain. Multiple reports may be selected from those nodes that summarize the requested data for the specified scope. Policies can be established for all objects contained within these domains. These reports and policy exceptions may be viewed on the screen, printed or exported to html or other file types.

The FastLane Suite plays a critical role in the preparation for Windows 2000. Many enterprises are faced with the requirement to clean up the existing network structure before upgrading to Windows 2000. The FastLane Suite provides the ability to:

- Report on user and groups memberships to allow for the removal of old accounts and inappropriate accounts, merging of groups, deletion of redundant groups, etc.
- Find exceptions to corporate policy and report on all users and their attributes - to allow for the correction of inconsistent naming conventions, correction of non-standard user attributes, correction of incorrect password options, etc.
- Report on hardware/software configuration, assessing which computers need to be replaced/upgraded for Windows 2000 - based on processor type, amount of RAM, hard disk size, operating system version, service pack number, etc., and

- Report on Microsoft Exchange mailboxes to allow for the deletion of unused mailboxes, mailboxes of previous employees or redundant mailboxes, correction of inconsistent data across the mailboxes, correction of inappropriate ACL (Access Control List) settings for the mailboxes, etc.

## Consolidation

### Key Considerations:

- What is your strategy to consolidate servers?
- Will your current servers handle the footprint of Windows 2000?
- Do your servers hold information that you need to migrate to the new servers?
- Do you need to perform a domain consolidation prior to the upgrade to Windows 2000?



Increased scalability is one of Windows 2000's major total cost-of-ownership (TCO) benefits, and part of achieving TCO savings remains the ability of companies to reduce the number of servers they manage through consolidation. Realizing the benefits of the increased scalability of Windows 2000 Server, GartnerGroup suggests that server TCO can be reduced by 30% by increasing the number of users per server from 75 to 250. However, in many organizations, massive data migration to much larger-capacity servers presents significant challenges.

### Key Consolidation Points:

- Data and security (ACLs, local groups, shares) must be preserved when moving data from a source server to a target server
- Servers may be incapable of being upgraded to Windows 2000 server because of a) insufficient disk space available, or b) insufficient processor capabilities
- A server consolidation done in conjunction with the deployment of Windows 2000 and AD can provide a compelling ROI value proposition
- Ensure preservation of all security settings and security principles during the migration of data
- Accommodate remote installation/operation of software
- Allow for on-line data migration to maintain end-user service levels

In smaller companies, with a single or few domains, the current NT 4 domain structure may be adequate in a Windows 2000 environment. However, domain consolidation could be essential in larger companies, where NT 4 has often been rolled out in a piecemeal, organic fashion that has left administrators with complex and hard-to-manage collections of domain structures and trust relationships. Some organizations have begun to re-model their NT 4 structures for various reasons, to do the following:

- Reduce redundant hard/software to support multiple master domain accounts
- Eliminate trust relationships that must be established and maintained by high-level Windows NT administrators
- Simplify Windows NT security and IT auditing

- Lower administration costs

For these organizations, the transition to the new NOS may run smoothly, since many required steps in an NT 4 domain consolidation are identical to those involved in a Windows 2000 migration.

Consolidating Windows NT domains *now* can reduce the overall challenges of a Windows 2000 upgrade. According to Microsoft, “Fewer domains created means fewer domains to migrate. In Windows [2000], there are no restrictions on restructuring within a domain. However, restructuring (merging domains, moving users between domains, and so on) is time-consuming.”

Therefore, by consolidating current Windows NT domains, an organization can determine enterprise-wide naming conventions – for user accounts, machine names, user groups, domain resources, etc. - thus eliminating time-consuming, often ‘political’ tasks during a Windows 2000 migration.

Planning and testing a consolidated domain architecture on Windows NT 4 will decrease the demand on IT resources during a Windows 2000 rollout.

In terms of network security, maintaining a reduced number of domains offers the ability to enhance security (fewer trust relationships) and reduce administrative costs.

### **The Quest Software Approach**

Quest Software’s approach to migrating data and security from a Windows NT Server to a Windows 2000 Server is enabled by FastLane Suite features that automate the migration and consolidation of data across partitions, across servers, and across domains while maintaining NTFS security, group and share points. Given the transitional state of the networks at this time, it is vital that the product transparently supports Windows NT and Windows 2000 servers.

Among the advanced features of the FastLane Suite that simplify and automate the server consolidation process are the following:

- Data migration is performed while the source server remains on-line and is accessible by the regular network users. This enables administrators to maintain normal service levels during the project. The FastLane Suite helps you perform each migration in stages rather than in a single inclusive process requiring extensive server downtime.
- The ability to intelligently analyze the data migration variables involved, makes the necessary Access Control List (ACL) adjustments, group re-mappings, and processes shares to ensure security integrity during the transfer of data from the source machine(s) to the target. In this way, administrators are saved much repetitive manual effort and network data security is preserved.
- A central console which allows the administrator to set up and manage multiple data migration jobs and which co-ordinates the software installation procedures for source and target machines. This architecture ensures for administrators that data travels the most direct network path between source and target - even when the console is not installed on the source or target computer. This makes the data migration process rapid and manageable for administrators.

Many of the components in the FastLane Suite’s consolidation solution operate as a Windows NT service. This means that data migration jobs are run without requiring an account to be logged in. Administrators often wish to securely schedule data migration jobs to run during off hours when there would be minimal impact to network users. In this way Quest offers administrators a secure and convenient data migration method.

## Migration

### Key Considerations

- What are your criteria for a migration tool/utility?
- Have you evaluated the different upgrade scenarios and determined which need to be supported?
- Have you determined where the data for AD will come from?
- What has to be accomplished as the part of the migration process? (consolidation/reorganization/upgrade)
- Has a project plan been created and validated?
- Are you aware of the logical steps within a Windows 2000-migration project plan? Are you aware of the implications of using SIDHistory during the migration?



Migration means moving users and groups, NT resources such as workstations, member servers, PDCs and BDCs into AD, as well as populating AD with data from multiple sources.

In small - to - medium sized organizations, Windows 2000's native AD Migration Tool (ADMT) could be sufficient to migrate data from the old system. However, the task will be considerably more complex in large enterprises, especially when populating an extended AD schema that may include objects from Microsoft Exchange, Human Resources databases or NDS (Novell Directory Service). Selectively populating this extended attribute set from multiple data sources is outside of the scope of native Microsoft tools, and more sophisticated third-party tools may be needed. It should be note that ADMT does not accommodate password migration; in this regard, the FastLane approach eliminates the chance of service level disruptions that could result from forcing password changes.

“For customers requiring greater sophistication and graphical tools, Microsoft is working with a number of Independent Software Vendors (ISVs) to ensure that there is also a healthy market for more fully featured third-party tools.”

- *Planning Migration from Windows NT to Windows 2000*,  
Microsoft Corp., 2000

Password security is never breached, as passwords remain encrypted during the migration.

### Key Migration Points:

There are two migration scenarios – ‘In-Place’, and ‘Restructure’, that both Microsoft and Quest provide.

- An In-Place Upgrade is the process of upgrading the Primary Domain Controller (PDC) and the BDCs of a Windows NT domain from the Windows NT Server to Windows 2000 Server domain controller.
  - With an In-Place Upgrade, the top-level domain must be moved first to AD, and then the child domains can be moved. A small network (less than 500 users), or environments with few NT domains, may be able to accommodate an In-Place upgrade scenario.
  - Large enterprises will probably use a combination of both migration scenarios. It is important to understand both scenarios to achieve the result of a properly and completely deployed AD.

- With a Restructure Upgrade, users are migrated incrementally to a pristine Windows 2000 environment without impacting the Windows NT production environment: it allows NT 4 domain structures and production environments to be preserved in the interim. Many customers have stated that the Windows deployment is a great opportunity to remove legacy problems that NT 4 domain structures have created.
  - The Restructure solution for large enterprises matches well with a risk-averse enterprise, allowing the creation of a clean and pristine AD environment and incrementally populating it with user accounts from the NT 4 environment. The NT 4 environment is operational and it can serve as a backup strategy.
  - Once the source environment is documented and the AD target forest structure is clearly defined, a more detailed project schedule can then be prepared: essentially, this can be described as ‘who gets migrated when and to where?’
  - It is vital to set rules. For instance, should a user’s NT 4 attributes be copied and set in AD? Also, should a user’s description, profile, login hours, login script and RAS permissions be copied? Should the new account have an expiry date? Should a user’s home directory path be copied? How are passwords handled? Should existing passwords be migrated or should they be randomly generated? Should a password change be enforced at first login?
  - Once a migration plan has been established, and the rules set has been communicated to the end-users and the help desk, the actual migrations can begin, either by using the provided Wizard or simply by dragging-and dropping users, groups and computers from the source NT 4 domains into the target AD domains and OUs.
  - When undertaking the kind of large-scale change that a Windows 2000 rollout requires, ensuring end-user service levels must be a primary goal. This means maintaining a degree of transparency, regardless of how significantly the system is being reconfigured during migration.

Therefore, network managers will need to choose a migration scenario. Should migration be done via In-Place upgrades followed by Restructuring, or by way of an incremental migration into a pristine AD forest? Should the Windows 2000 domains be in mixed mode or native mode? Can SID History be leveraged, or will it be better to re-ACL?

### **The Quest Software Approach:**

1. Maintain control of the large number of objects being migrated to AD. For large enterprises, thousands of objects must be migrated. This process is impeded if migrations are not centrally managed. Audit of all migration activities is required to ensure that end user service levels are met.
2. Populate the additional attributes of AD objects with data from other data stores (e.g. HR databases, payroll database, telephone lists, etc.).
3. GartnerGroup suggests that there is an 80% probability that 60% of enterprise customers will not properly deploy AD the first time and that they will need to either re-deploy or significantly restructure their AD forest within 18 months. Therefore, anticipate ongoing AD forest pruning and grafting.

(Note: Many migrations to AD may be to domains running in mixed mode, or could also be inter-forest (across AD domains in a single AD forest). Both of the scenarios, which are common, are such that SIDHistory is not an option. In order to maintain end user service levels (access to server-based resources, mailboxes, etc.) extensive re-ACLing is required. This re-

ACLing process must be scheduled, distributed and non-destructive in order to be a viable enterprise solution).

### The FastLane Suite Delivers:

1. The incremental migration of users, groups and computers to AD: the unique capability of the FastLane Suite to track those migrations and allow for detailed auditing and completely granular 'undos'
2. Project-based migrations and drag and drop migrations
3. The FastLane Suite can also select a previous migration project file and show the reversal of a subset of that migration project
4. The population of the extended AD attribute set with data from a secondary data source as part of the migration
5. Ongoing pruning and grafting of the AD forest
6. Mixed or native migrations, with/without SIDHistory, inter/intra forest
7. Password migration

The migration's success depends on maintaining end-user service levels with minimum disruption. To do so requires the addition of the user's new SID (Security Identifier) to all of the resources that exist in the network, including files, shares, computers, and groups. What is required is a centrally managed automated method.

There are several reasons why network administrators choose to use an automated application, as it:

- Drastically reduces the manual effort and costs
- Reduces the risk of network downtime and impact on end-user service levels
- Reduces the human error factor
- Provides comprehensive project tracking and auditing of all actions taken
- Allows for staged migrations with fall back to the original accounts

## Clean-Up

### Key Considerations

- How will you decommission the old Windows NT domains as you move to Windows 2000?
- How will you disable/delete old Windows NT accounts that have been migrated and are no longer required?
- How will you clean out old NT ACE (Access Control Entries) on resources?
- How will you decommission old servers as you move to Windows 2000? How will you remove redundant delegation products from the network?



'Clean-Up' is a critical migration phase, and one that is often ignored – yet it is essential to maintaining the health of the new environment.

### Key Clean-Up Points

- Disable and delete old NT accounts & SIDs

- Decommission redundant infrastructure - Windows NT delegation, NT servers, domains, etc.
- Decommission old servers as you move to Windows 2000
- Remove redundant delegation products from the network

Without proper tools, Clean-Up can be a difficult task. Experience from major NT4 domain consolidation projects shows that an enterprise network typically includes an average of 3,000 ACLs per user. The average Global 2000 customer has 27,000 users, which means administrators must manage approximately 90 million extended objects. In other words, whether the migration happens with or without SIDHistory, there is still a tremendous amount of Clean-Up required - on every machine and in every directory, right down to the share and file level.

### **The Quest Software Approach**

Clean-Up involves first disabling and deleting old accounts, and removing their associated SIDs from across the network. "Old" SIDs must be removed from resources in the production environment to prevent effectively being deleted while user access to the resource is via SID History. However, caution must be exercised: inherent security risks may exist with SIDHistory. For example, users may have multiple User Unknown messages in groups and ACLs (e.g., a source account having had full access to a resource under NT 4 - and who received lesser rights under Windows 2000 - will still have full access to the resource thanks to their old NT 4 access).

The next step in Clean-Up involves decommissioning redundant or obsolete infrastructure, including the old NT 4 delegation model and NT servers whose data has been migrated. Specialized tools may be desirable for converting PDCs and BDCs to member servers in a new Windows 2000 domain, an essential task that is not easily done natively. Once this Clean-Up is complete and the end-state is reached, old hardware from the source environment can be reclaimed. Old user domains may be decommissioned once the PDC disappears, then trusts will need to be cleaned up. Next, servers that are no longer required can be repurposed for the Windows 2000 environment as additional member servers.

### **The FastLane Suite Delivers:**

1. Clean up the resource security setting on servers (ACLs, local groups, Windows NT profiles, and user rights). Incidences of users' SIDs, that are propagated around a network, must be found (regardless of location) and replaced with the new user SID. Additionally, domain controllers (PDC/BDCs) must maintain their file permissions, security integrity and share structure when being re-deployed in the target AD domain.
2. Manage both the SIDHistory and re-ACL post-migration Clean-Up process. This includes scheduling Clean-Up jobs to be run on resources that update all of the resource security settings with the new user SID: this means that the security settings on all resources will only reference the user's new AD account, facilitating system auditing, security reporting, and ongoing administration of resources.
3. Quest tools automate the conversion of Windows NT 4 PDCs/BDCs to either Windows 2000 DCs or member servers in the new Windows 2000 domain, while preserving all security settings (ACLs, Local Groups, and Shares).

## Administration

### Key Considerations

- How will you keep your Windows NT policies in place as you move to Windows 2000?
- Have you assessed products for the ongoing management of a mixed Windows NT/2000 network and the eventual pure Windows 2000 network?
- How do you simplify and automate administrative processes during the co-existence period with Windows 2000?
- Do you foresee the need for ongoing pruning and grafting of the AD Tree (OU to OU, domain to domain)?
- Will you continue to upgrade your servers in the future to take advantage of new hardware improvements?
- How do you plan to automate administrative processes during the coexistence period with Windows 2000?



In terms of timing, ongoing infrastructure administration and management of a “pure” Windows 2000 environment may not be in the immediate future. Nevertheless, some administration issues - security and policy enforcement, for example - will continue to remain paramount. So will attempts to simplify and automate tasks, which, when successful, provide time and resource savings. Lastly, creating and maintaining a unified administrative structure - all the way through the evolution from a pure NT 4 to a mixed NT 4-and-Windows 2000 environment, and finally to a “pure” Windows 2000 environment - will save time and reduce costs.

### Key Administration Points

- Apply security & policy enforcement practices
- Report on security integrity
- Identify security violations
- Review exceptions to administrative policy
- Simplify and automate administration

Delegation of administration has come a long way in Windows 2000, and once again, the native delegation will likely be more than adequate for many customers. But native delegation requires choices about the OU hierarchy. Windows 2000 objects can exist in a single OU only, and OUs cannot span domains or forests.

### The Quest Software Approach

The FastLane Suite delivers directory-enabled solutions to assist in the management of AD native delegation. This delivers simplified mechanisms to define role-based administration, which allows for rapid and effective assignment of AD rights and significantly reduces the costs of AD management.

The FastLane process applies to the ongoing pruning and grafting of AD structure - facilitating business reorganizations, mergers and acquisitions and other AD reorganizations.

#### **The FastLane Suite Delivers**

- Improves IT service levels by creating a more efficient and flexible administrative model for Microsoft environments
- Creates a functional AD-like structure for the planning and migration to Windows 2000

## **Summary**

According to Microsoft, “Active Directory is an essential and inseparable part of the Windows 2000 network architecture...” Therefore, an effective solution for deploying Windows 2000 must be based on a firm understanding of Active Directory. Quest Software maintains that many of the most significant benefits of Windows 2000, many of which have been discussed in this technical brief, *cannot* be attained *without a properly and fully deployed AD*. To that end, Quest has developed field-tested methodologies and tools that accommodate and promote the interrelated benefits of both AD and Windows 2000.

The introduction of Windows 2000 has increased awareness of a directory’s critical role in enterprise management. Since 1993, Quest Software’s FastLane Migrator™ has helped hundreds of major organizations simplify the management of their enterprises. Quest’s global leadership position stems from focusing on enterprise-wide ‘Directory Management’. Prominent enterprise issues, such as scalability, security and reliability, comprise the foundation of our task-oriented suite of products.

This paper has offered a selected overview of Windows NT, Windows 2000 and AD with the purpose of demonstrating the applicability and diligence of the FastLane process, an integrated and globally supported approach to Windows 2000 deployment.

To summarize Quest Software’s five-step approach to Windows 2000 deployment:

#### **Plan**

- Assess your current Windows NT and Exchange environments
- Plan and budget the deployment/implementation processes
- Build a hierarchy for AD on Windows NT

#### **Consolidation**

- Consolidate Windows NT user and resource domains
- Consolidate servers and data
- Consolidate administrative structure

#### **Migrate**

- Migrate Windows NT users and groups
- Migrate Windows NT resources
- Fully populate AD's extended schema with objects and attributes from other sources

#### **Clean-Up**

- Disable and delete old accounts & SIDs
- Decommission redundant infrastructure - Windows NT delegation, NT servers, domains, etc.



### **Administration**

- Apply Security & Policy Enforcement practices
- Establish a role-based administrative structure
- Review exceptions to administrative policy
- Simplify and automate administration

## **About Quest Software**

Quest Software, Inc. is a leading provider of performance management solutions designed to maintain the integrity of mission-critical business transactions and maximize the performance of enterprise applications. Our solutions address the needs of today's 24x7x365 businesses where demands on the information technology infrastructure are high and tolerance for downtime is low. The Internet has propagated the expectation of instant access to information, and Quest delivers the solutions necessary to meet this demand.

Founded in 1987, Quest Software now helps more than 100,000 users achieve the best possible performance from their enterprise systems so the end user experience is a positive one. Based in Irvine, California, Quest Software has offices worldwide and over 1,500 employees. For more information, visit [www.quest.com](http://www.quest.com).



8001 Irvine Center Drive  
Irvine, CA 92618  
Email: [info@quest.com](mailto:info@quest.com)  
U.S. and Canada: 949.754.8000  
UK: +44.1628.601000  
Germany: +49.211.770967.0  
Australia: +61.3.9811.8000  
France: +33.1.4131.9696  
Scandinavia: +45.7021.7050  
Benelux: +31.204.91.9491

All content Copyright© 2001, Quest Software, Inc. The information in this publication is furnished for information use only and is subject to change without notice. Quest Software, Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in this publication. Other product or company names mentioned herein may be the trademarks of their respective owners.

FastLane is a registered trademark of Quest Software, Inc. FastLane Suite, FastLane Reporter and FastLane Migrator are trademarks of Quest Software, Inc.

## Glossary<sup>3</sup>

### Access Control Entry – ACE

An object such as a user or group that is present on an Access Control List.

### Access Control List – ACL

A description of security permissions applied to an object, property or resource. An ACL normally includes membership (ACEs) and the associated actions or manipulations that each member can perform on the item.

### Active Directory

The Windows 2000 directory service. This replaces the Security Accounts Manager (SAM) in Windows NT 4. AD consists of a forest, domain(s), organization units, containers and objects. Different classes of objects can be represented within AD including users, groups, computers, printers and applications. The use of AD is governed by its schema.

### Active Directory Services Interfaces – ADSI

A directory service abstraction interface that allows programming languages that are compatible with the Component Object Model (COM), such as Visual Basic, VBScript, JavaScript, C, and C++ to make common directory calls to an underlying directory service. ADSI providers include Lightweight Directory Access Protocol (LDAP), NDS, Bindery and Windows NT (SAM). Programmers and system administrators normally use ADSI to automate or script the bulk manipulation of directory entries.

### Domain controller

A server that can authenticate users for a domain. There must be at least one domain controller in each domain within the forest. Each domain controller holds a complete replica of the domain naming context that the server is in and a complete replica of the configuration and schema naming contexts for the forest.

### Domain mode

An AD domain can be in either *mixed-mode* or *native-mode*. In mixed-mode, the domain is restricted to limitations (such as 40,000 objects) imposed by the Windows NT 4 domain model. However, Windows 2000 domain controllers and Windows NT 4 backup domain controller can seamlessly co-exist within the domain without problems. Switching to native-mode, which is irreversible, allows the directory to scale up to millions of objects and overcome the constraints of the legacy SAM, but requires that all domain controllers be upgraded to Windows 2000. A domain in native-mode allows for rich group creation and nesting, which is advantageous to Exchange 2000.

Note that Windows NT 4 member servers can still exist within a native-mode domain. Additionally, clients do not have to be upgraded before the domain mode is switched.

### Domain Name Services - DNS

A major standards-based protocol that allows clients and servers to resolve names into Internet Protocol (IP) addresses and vice versa. Windows 2000 extends this concept even further by

---

<sup>3</sup> Based on 'Microsoft Windows 2000 and Microsoft Exchange 2000 Server Terminology Primer'. Microsoft Corp., 1999.

supplying a Dynamic DNS (DDNS) service that enables clients and servers to automatically register themselves in the database without needing administrators to manually define records.

### **Domain tree**

A collection of domains that have a contiguous namespace, such as *fastlane.com*, *dog.fastlane.com* and *cat.fastlane.com*. Domains within the forest that do not have the same hierarchical domain name are located in a different domain tree. A *disjoint namespace* is the term used to describe the relationship between different domain trees in the forest.

### **Forest**

A collection of domains and domain trees. The implicit name of the forest is the name of the first domain installed. All domain controllers within a forest share the same configuration and schema naming contexts.

### **Group**

An object defined in AD that contains members of other objects such as users, contacts and possibly other groups. A group may be of type *distribution* or *security* depending on the requirement, and have a scope of either local, domain, or universal.

### **Lightweight Directory Access Protocol – LDAP**

A standards-based protocol that can be used to interact with conformant directory services.

### **Namespace**

A logical collection of resources that can be managed as a single unit. Within AD, a domain defines a namespace.

### **Schema**

The metadata (data about data) that describes the use of objects within a given structure. In AD, the schema governs the type of objects that can exist and the mandatory and optional attributes of each object. Windows 2000 AD has an extensible schema that allows third parties to create their own object classes. Schemas also exist for other components such as the message transfer agent and information store in Exchange Server.

### **User**

In AD, this is a security principal (a user who can log on to the domain). A user may have an e-mail address and/or an Exchange mailbox, making the object mail-enabled and/or mailbox-enabled, respectively.