Windows 2000 Migration:
Best Practices

Windows 2000 Migration: Best Practices

White Paper

August 25, 2000

Contents

The purpose of this document is to provide an introduction to Windows 2000 migration concepts, scenarios, common issues, and best practices. This document assumes you have an administrator-level understanding of Windows networking architecture and domain migration concepts.

First Edition

NetIQ Corporation provides this document "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. Some states do not allow disclaimers of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This document and the software described in this document are furnished under a license agreement or a non-disclosure agreement and may be used only in accordance with the terms of the agreement. This document may not be lent, sold, or given away without the written permission of NetIQ Corporation. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, with the prior written consent of NetIQ Corporation. Companies, names, and data used in this document are fictitious unless otherwise noted.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of the document. NetIQ Corporation may make improvements in and / or changes to the products described in this document at any time.

General Terminology

This section provides some preliminary domain migration concepts and terminology you should know before reading this document.

Clean and pristine
Term used to describe a brand new Windows 2000 native mode domain that will be the target of a migration.

Upgrade in place
A migration strategy where the affected domain is simply upgraded either before or instead of a domain migration.

Inter-forest migration
Term used to describe domain migration between either two domains residing in different Windows 2000 forests or a domain migration from Windows NT 4 to Windows 2000.

Intra-forest migration
Term used to describe a domain migration between two domains in the same forest, with a native mode target. Special conditions apply to intra-forest migration, such as the source object being moved (deleted in the source and re-created on the target domain) to the target domain. In this case, the GUID is retained and the source object SID is appended to the SID History of the target object.

Mixed mode domain
A Windows 2000 domain that is running in Windows NT 4 compatibility mode. Customers typically run in this mode because they have Windows NT 4 Backup Domain Controllers (often running applications that make an upgrade difficult). Mixed mode domains use the Windows NT 4 single-master model for writes to the directory.

Native mode domain
A Windows 2000 domain that is running the Windows 2000 native Kerberos-based authentication system. Native mode domains are multi-master for purposes of directory updates. They also support SID History and intra-forest moves via MoveObject.

SID History
An Active Directory attribute that is often used in migrations to native mode. Its function is to retain SIDs in the access token from other domains. SID History is a multi-valued attribute, meaning that it can contain more than one Sid from previous domains. This attribute is only accessible in native mode target domains. For more information and a detailed list of requirements, please see “Understanding SID History” on page 14.

MoveObject
An Active Directory operation that involves the source object being moved (deleted in the source and created on the target domain) to the target domain. In this case, the GUID is retained and the source object SID is appended to the SID History of the target object. This process allows all properties of the object to be preserved.

Understanding Your Migration Options

What is driving organizations to migrate? Companies are performing migrations for a variety of reasons:

- New technology, such as Windows 2000 or Exchange 2000
- Business unit re-organizations, mergers, acquisitions and spin-offs
- Administrative restructuring driven by a need to simplify the environment

Once you have decided to migrate to the latest technology base, what are your options for migrating to Windows 2000? There are a number of general strategies for migrating to Windows 2000 and restructuring domains:

Upgrade in place and leave domain structure intact

Upgrade in place to Windows 2000 and then migrate intra-forest

The most common reasons for upgrading in this fashion is the organization only has one Windows NT account authentication domain or there is a big need to maintain their current passwords (note that Domain Migration Administrator from NetIQ will copy passwords between domains). On the downside, there is very little ability to rollback changes and the current environment must be in a state that is compatible with the desired structure for Windows 2000.

Upgrade in place and collapse resource domains

This scenario is common in environments where the resource domain structure can be better managed by collapsing resources into organizational units (OUs) in the migrated account domain structure. Without a tool to automate this process—changing machines domain affiliations and creating a new computer account in Windows 2000 in the desired OU—this would not be a viable option. The ActiveAgent technology in NetIQ Domain Migration Administrator copies the computer accounts to the Windows 2000 domain and places them in the correct OU, then the systems are joined to the new domain.

Migrate Windows NT 4 or Novell environment to a clean and pristine Windows 2000 domain

This scenario is used when customers take the opportunity to restructure their domain environment around the capabilities of the Active Directory. A common phrase used to describe this operation is a parallel environment. New Windows 2000 Domain Controllers (DCs) holding the Active Directory structure are built alongside the existing infrastructure. User accounts and groups are migrated to the new environment, and existing workstations are joined to the new domain by the ActiveAgent technology in NetIQ Domain Migration Administrator. In some cases, existing Backup Domain Controllers (BDCs) in the source Windows NT 4 domain cannot be quickly upgraded to Windows 2000 due to the risk associated with client-server applications installed on those machines. The parallel environment allows Administrators to take advantage of the new features in the Active Directory while users still access resources in the old environment.

Many customers require guidance on designing and executing their migration strategy. Here are some helpful questions for determining customer migration needs:

- When will the migration begin?
- When is it expected to conclude?
- How many users are being migrated?
- How many domains are planned?
- How many forests are planned?
- What does the current domain structure look like?
- Will the target domain be mixed mode or native mode?
- Will SID History be used?
- Will re-ACLing be used for files, shares, user profiles, etc?
- Are other platforms (NetWare, Banyan, etc.) being migrated to Windows 2000 in conjunction with the domain restructuring?
- Will the DNS reside on Unix or on Windows 2000?

Migration Scenarios

This document addresses different business scenarios based on the migration operations previously described. The scenarios are based on actual and planned migrations:

- Migration from Novell NetWare / NDS
- Single account domain migration
- Resource domain consolidation
- Multiple account domain migration

The following two NetIQ products are the tools used in the migration scenarios:

- NetIQ Domain Migration Administrator (DMA): A client-only tool used to migrate user IDs, member servers, member workstations, trusts and other resources from either a Windows NT 4.0 to a Windows 2000 environment. Employs NetIQ technology also delivered in the Microsoft Active Directory Migration Tool (ADMT).
- NetIQ NetWare Migrator: Migrates users from NetWare Bindery or NDS to Windows 2000. Multiple source bindery and / or NDS accounts can be merged into Windows 2000. Copies files and associated permissions to Windows 2000 file servers.

Migration from Novell NetWare/NDS

A medium-sized legal firm has two main offices and two remote offices. The firm has placed a Windows 2000 server in each location and has completed design of their Active Directory structure. Each office has a NetWare 4.11 server (running NDS), and the main offices each have a NetWare 3.12 server (running bindery). The offices are connected by high-speed links.

The primary application running on the NetWare 4.11 servers had been an SQL database system. The database system has been crossed over to Windows 2000 and the users of that system have completed their changeover.

One design decision made early on was to create a new tree structure in Active Directory rather than use the tree structure in their existing NDS environment. The IT staff had learned through their own experience how to best organize the tree and they wanted to begin with a clean structure.

Since users needed to be migrated to Active Directory and files to Windows 2000 file servers, the NetWare servers would not be needed post-migration.

An OU was then created in Active Directory for the bindery user objects. The bindery-based users were migrated to this OU, and then cleanup was performed. Similarly, an OU was created for NDS user objects, and then cleanup was done after the user objects were migrated from NDS to Active Directory.

Files were copied with permissions to file servers located in the various offices. Server consolidation was relatively easy since newer server-class computers were being used for the Windows 2000 file servers.

Where necessary, Windows 2000 login scripts were modified to replace the file accesses that had been designated in the NetWare login scripts.

Once migration had been done, the file permissions on the NetWare servers were set to read-only so they could find any dangling pointers to NetWare-hosted files. After these were cleaned up, the NetWare servers were removed from the network so that any additional references could be discovered.

Files didn't have to be erased during the migration process since the migration was accomplished in parallel with the Windows 2000 environment.

Single Account Domain Migration

A small manufacturing company is currently on a Windows NT 4 environment, using Exchange for their email application. They are planning their migration to Windows 2000 now since they are very interested in moving to Exchange 2000 as soon as it becomes available.

Because they are planning for Exchange 2000, they are looking at migrating away from their Windows NT 4 infrastructure to a clean and pristine environment. They had originally planned to build the native mode Windows 2000 forest using ClonePrincipal until Microsoft released the Active Directory Migration Tool (ADMT). After reviewing the ADMT features, they decided to purchase NetIQ Domain Migration Administrator for the password migration capabilities. DMA also offers enhanced reporting, better performance and project-tracking capabilities. In addition to the functionality of ADMT, DMA has the ability to test a migration and report on what would have happened before any changes are committed.

The entire migration project will encompass 1,500 users in four sites (three office spaces and one manufacturing facility). The DMA project wizard will allow the migration team to track the progress of the migration at the four individual sites (translated profiles, security translation not completed, failed workstations, etc) as well as run weekly reports for the entire domain to assess adherence to their strict schedule (migrated users, migrated groups).

The migration team will create separate migration projects containing the users, groups, and workstations at each site to be migrated. The DMA wizard allows you to select the groups that identify each site, enumerate the members of the groups, and load groups and users into the migration project.

The initial migration plan was to take advantage of the SID History attribute in the Active Directory so security would not have to be translated. After a more careful evaluation, however, the migration plan was modified to include a SID History cleanup to prevent complications in the Directory from large Kerberos authentication packets. (For more information, see TechNet article Q263693). NetIQ Domain Migration Administrator provides a wizard for this operation to simplify this process.

In the first and second sites, the users normally shut down their workstations when they leave for the evening. In preparation for the weekend migration, users were instructed to log off their machines without shutting down. This will facilitate the profile translation, domain membership change and subsequent reboot of the local machine by the ActiveAgent technology. In the third site to be migrated, the systems are laptops that travel with outside employees. These employees were contacted so other arrangements could be made -- some were able to dock their laptops for the weekend, others returned the laptop for an upgrade due to hardware requirements with their desktop rollout.

Because they could install the ActiveAgent on multiple machines simultaneously for security translation tasks and domain membership change, the migration plan was designed around a five-day cycle for each site.

- Two days were allotted for testing of the environment: verification of permissions for the migration account, testing of WINS and DNS name resolution and final identification of workstations to be migrated.
- One day was allotted for the execution of the migration project: user accounts were migrated; then groups and group memberships; and workstations were the last step.
- Two days were allotted for failed task resolution (machines not online) and testing. A failed tasks report identified the migration tasks that needed to be repeated after the cause was identified and the problem was resolved.

In this particular case, additional user IDs were created with known passwords and added to groups being migrated so the migration team could test file access.

The SID History clean-up operation was then executed after all sites were successfully migrated. Backups were made of all file servers before executing the operation. The DMA wizard identified the accounts in the Active Directory with SID History attributes and then translated security for those accounts so permissions accurately reflected the new Windows 2000 account and SID.

Resource Domain Consolidation

An insurance company is currently operating in a Windows NT 4 environment. They have a single master account domain with multiple resource domains for each remote site. Their goal for migrating to Windows 2000 is to reduce administrative costs by collapsing the resource domains into Organization Units in the Windows 2000 domain.

Before evaluating any migration tools, the existing Windows NT 4 PDC was upgraded to Windows 2000. They originally planned to change the domain membership of 130 resource servers manually until they discovered that several servers in different resource domains had unacceptable computer names.

An engineer was brought on site to assist with the migration plan and develop guidelines for consistently naming machines, deploying the naming convention and joining the systems to the new domain. Because of her experience with NetIQ Domain Migration Administrator, she knew that the Computer Rename wizard would change system names and implement the naming standard. The engineer established a naming standard based on location and server role, which was implemented before the systems were migrated to the new domain to eliminate confusion.

A target OU was specified for systems from each resource domain in the Computer Migration wizard. By creating the account and dispatching the ActiveAgent to change the domain affiliation and reboot the machine, she simplified the migration process. The engineer did not have to manually change the domain membership of each machine, and then move each computer to a specific OU through the AD Users and Computers snap-in.

Post-migration analysis further illustrated the operation efficiency. The two reboots required for the name change and the domain membership change amounted to only a fraction of the scheduled downtime. Since the naming standard was in place, trouble tickets were more quickly routed to the appropriate administrator for resolution.

The engineer left behind a document detailing the naming standard for systems, though the LAN administrator indicated there was no way to force administrators to follow the standard. Because of her familiarity with NetIQ products, she was then able to demonstrate the NetIQ Directory and Resource Administrator product, which allows an Administrator to delegate administrative tasks while enforcing business rules and policy on the delegated environment. DRA enabled the LAN administrator to not only enforce a new naming standard for machines, but also restrict the OU where computer accounts could be created.

Multiple Account Domain Migration

A large financial services company is preparing for an enterprise-wide deployment of Windows 2000. In contrast to many smaller operations, every step of the process must be detailed.

The Windows 2000 migration plan will incorporate a parallel environment in order to minimize the amount of service disruption and facilitate complete rollback of unforeseen incidents. This will be achieved by keeping most of the Windows NT 4 environment intact throughout the migration period. Except for Windows NT 4 application servers that have to be moved to the Windows 2000, the environment will not be rebuilt anew in the Windows 2000 environment.

This scenario outlines a five-phase migration plan for the business units to migrate to Windows 2000 from the existing Windows NT 4.0 and / or Novell NetWare environment(s). The plans take into account the differences in the organization, operations and architecture of the existing Windows NT 4.0 and NDS environments.

The current state of the Windows NT 4.0 environment will be analyzed and mapped to the desired Windows 2000 environment in the post-migration period. The migration process will be executed in five phases. For more information, see “Recommended Steps for Windows 2000 Migration” on page 10:

- Phase 1: Research, Planning and Requirement Definition
- Phase 2: Test / Trial Migration, Contingency Planning
- Phase 3: Domain and Server Migration
- Phase 4: Desktop / Workstation Migration
- Phase 5: Post Migration Testing and Clean Up

The scope of this scenario will cover design principles, migration tools setup and configurations. The project plan will include migration of master and resource domains including user IDs, security settings, disk shares, printers, profiles, logon scripts, exchange mail, remote access, dynamic DNS and WINS.

In summary, the migration will involve the creation of a new Windows 2000 infrastructure in a parallel environment to the existing Windows NT 4 infrastructure. The migration process will be a collaborative effort between enterprise level administrators and business unit administrators. NetIQ Domain Migration Administrator will be used for the migration

Windows NT 4.0 Pre-Migration Environment

The Windows NT 4 environment consisted of six Trusted Master Account Domains; five of which were in a Multiple Master / Resource configuration; the other was a Master account domain in Single Master configuration.

Domain Architecture and Trust Configurations

The environment contained an estimated 200 resource domains globally. Enterprise resources, such as Exchange, were in the master account domains. Business-specific resources, such as file and print services and application servers, resided in the resource domains.

Name Service Structure (WINS/DNS)

The WINS servers in the Windows NT 4.0 environment will be upgraded in place to Windows 2000 to leverage better performance in supporting both the Windows NT 4.0 and Windows 2000 environment. The performance will come from WINS service enhancements and improved IP stack in Windows 2000.

Resource Structure (Exchange, File and Print, Application Servers)

Exchange Servers currently reside in four of the five master account domains. File and Print and Application servers reside in resource domains that trust into the global multiple master domains.

The infrastructure described above must be inventoried, divided and delegated to specific business units group that will take be responsible for migrating them to Windows 2000. The management structures of the environments vary. Several of the account domains have a distributed management structure with most of the operations handled by business units. One of the account domains has a very strict hierarchical structure. NetIQ Domain Migration Administrator provides the flexibility to allow all domains to configure their migration project independently.

The assessment of files, profile location, etc. will be handled by DMA. The reporting module will gather information from the servers in the resource domains and compile it in a central location. These reports will be used to determine which servers need to be migrated with specific business units. In addition, service account information will be gathered to ensure service is not interrupted during the upgrade.

Windows 2000 Post-Migration Environment

The Windows 2000 environment will consist of a Place Holder domain and location trees. Business unit OUs and resource domains will be contained within the trees -- all bound by transitive trusts. This will allow resources to be shared seamlessly across the world and facilitate distributed administration.

All enterprise and business-specific resources will be contained in the resource domains. The domains will be divided into Organizational Units (OU) to facilitate distributed administration.

Name Service Structure (WINS/DNS)

The WINS environment will remain in the pre-migration state until all Windows NT 4.0 domain and resources have been migrated to Windows 2000.

The WINS servers in the Windows NT 4.0 environment will be upgraded in place to Windows 2000 to leverage better performance in supporting both the Windows NT 4.0 and Windows 2000 environment.

Dynamic DNS is required by Windows 2000. The networking group will provide infrastructure guidelines for the dynamic DNS implementation.

The DMA Reporting Wizard will be used to gather service information from the remote servers. This information will allow the identification of the existing WINS servers for upgrade planning.

Resource Structure (Exchange, File and Print, Application Servers)

Exchange, File and Print and Application servers will reside in the respective OU of the business units. DMA will create the new system account in the Windows 2000 domain and change the domain membership of the servers (including the reboot). The destination OU can be specified in the migration project to ensure the users, groups, and servers are all located in the business unit OU.

Implementation Strategy for Windows 2000 Migrations

NetIQ Directory and Resource Administrator manages the existing Windows NT 4 infrastructure. This product allows administrators to create ActiveViews (logical units for organizing domain objects) and delegate specific administrative tasks to users in the enterprise. This facilitates delegated administration and auditing of all administrative operations.

Design Principles

The following principles will guide the migration process in all areas where the planning and instructions are insufficient:

- Top-level business OU will exist consistently in all regional domains.
- Where applicable, existing DRA ActiveViews will map into top-level business OU.
- Full rollback capability will be available throughout the migration process.
- Migration process will not disrupt business operations.
- Migration will be project-based.
- Migration assessment reporting will be available at all time.
- A parallel environment will be created except for existing WINS servers.
- Immediate re-ACLing will be used instead of SID migration.
- Migration will be done in a distributed manner.
- Security and naming standards will be applied and enforced.

Migration Process Implementation Overview

The migration process will consists of collaboration work between Master Domain Administrators and business unit resource domain administrators as follows:

- For distributed management environments, resource domain administrators will have Directory and Resource Administrator delegated rights in the master account domains and full administrative rights in their source resource domains.
- For centrally managed environments, rights will be delegated using Directory and Resource Administrator. Very few people will actually have Domain or Enterprise Admin accounts to both source resource domains and source master account domain environments.

- Resource domains administrators will use the DMA tool to create a Migration Project (a migration project is an actual migration where the transactions are not immediately applied but saved to an Access database to be executed / applied at a later time by an ID having full administrative rights in both master and resource domains). The migration project will contain the users, groups and computers they wish to migrate and settings related to the migration process, such as renaming objects.
- They will save the file project file and send it to the team actually running and approving the migration projects. This team will have administrator rights to all objects in both the master and resource domains.
- Project will be tested and assessment reports will be generated for review.
- Once the migration project has been approved -- that project will run in *Migrate Now* mode instead of *Testing* mode.
- Upon completing the bulk of the migration process, they will use the Windows 2000 Server resource kit, scripts, and other tools for special case migrations and clean up as necessary.

Migration Tool Initial Configuration and Requirements

- A two-way trust between source Windows NT 4.0 master domain and the target Windows 2000 domain.
- A one-way trust must between source resource domain and the target Windows 2000 domain.
- Domain Migration Administrator (DMA) installed on a Windows 2000 member server.
- Team running the migration must be given administrator access on all systems and domains involved in the migration.
- Domain Administrative rights in both source and target domain environment is required to execute migration project file.
- DRA delegation rights must be given to resource domain administrators (or ACL permission set on OUs) in the target Windows 2000 domain. This is needed so administrators of resource domains can still manage their users after the migration.

Domain/Trust Configuration

All source Windows NT 4.0 domain environments will trust the target Windows 2000 domain during the migration -- facilitating the migration from the Windows NT 4.0 environment to the delegated Windows 2000 OU.

Migrating Objects

The recommended order for Windows NT 4.0 objects to be migrated:

- Groups Account and their members (Users) by DMA.
- Security translation on all ACLs.
- User workstation machine accounts migration and local profile translation by DMA.
- Service account migration.
- Exchange server security translation.
- Special case migrations with other utilities and manpower.
  - Application migration to Windows 2000 and new domain.
  - Windows 9x platforms migration.
  - Logon script changes needed for new domain structure.

The DMA product will track failed workstation migration or failed security translation for retry after the problem is resolved. Common points of failure are insufficient permissions (Domain Admins group is no longer in the local Administrator group of the system) or name resolution (WINS database did not have an entry for the system).

Recommended Steps for Windows 2000 Migration

This section provides the recommended steps for an organization migrating from Windows NT 4 to Windows 2000.

Phase 1: Research, Planning and Requirement Definition

Inventory All the Resources in Your Windows NT 4.0 Environment

- Domain environment configurations (network protocols, trusts, profiles, home shares, scripts etc.).
- Servers and workstations to be migrated (applications and server locations).
- Users and groups to be migrated.
- Positions of DCs over data highway network.

Domain Migration Administrator has reports available to identify location of profiles, status of domain trusts, group membership, user account conflicts between domains and more. In addition, the existing DRA installation can be used for ActiveView membership to model the migration products.

Define the Windows 2000 Features You Plan to Use in Addition the Global Ones

- Categorize features as *must haves* and *like to haves.* For more information see “Partial List of Windows 2000 Technologies” on page 16.
- Define the timeframe in which you wish to complete the migration.
- Define milestones dates and goals for migration.
- Determine required training for support staff and end users.

Tools for Research and Planning

- The Windows 2000 Server Resource Kit and the Windows 2000 Server Deployment Guide available on the Microsoft Web Site at http://www.microsoft.com/windows2000 are very useful.
- The Domain Migration Administrator and Directory and Resource Administrator reporting tools can be used to inventory users and assess security settings.
- The Directory and Resource Administrator ability to create ActiveViews allows you to plan your OU structure and your migration projects.

Training for IT Staff

- Windows 2000 training for your IT staff is required in order to research your environment and plan your migration.
- Classes are available from Microsoft and their partners.
- Web-based classes are also available from various vendors (Learn2.com, Pinacor.com)

Phase 2: Test/Trial Migration, Contingency Planning

This is probably the most important phase of the migration process.

Prepare Your Test and Production Environment

- All hardware and software should be checked for Windows 2000 compatibility.
- Non-compliant packages must be upgraded.
- Upgrade RAM in servers and workstations as required by Microsoft.
- Apply latest Windows 2000 service pack.

Use DMA Tool to Test and Plan Trial Migration and Contingency

The product has database modeling capabilities as well as a test (no change) mode for preparation. Most connectivity and permissions problems can be identified with the test mode. Note that all machines must be online for testing and migration. In addition, users must be logged off for local profile translation.

The NetIQ Administration product line consists of the following modules:

Directory and Resource Administrator
: Provides distributed administration of user accounts, groups, and system resources increasing security and reducing network costs with automated, policy-based administration and extensive auditing and reporting.

Exchange Administrator
: Provides distributed administration of Microsoft Exchange mailboxes and distribution lists lowering network cost through automated policy based Exchange administration.

Domain Migration Administrator
: Migrates user accounts, groups, member servers, workstations, user rights and other components between Windows NT and Windows 2000 domains. Preserves existing resources and can operate without disrupting end users.

NetIQ NetWare Migrator
: Migrates user accounts from NetWare Bindery or NDS to Windows 2000.

File and Storage Administrator
: Allows you to proactively manage file and share permissions and properties across servers. This product also provides extensive reporting on disk space utilization, file statistics, and security reference data. File and Storage Administrator dramatically reduces the time, effort, and resources required to secure and administer the Windows NT 4.0 and Windows 2000 file system.

Testing Requirements

The trial migration environment should contain a representative structure of the production Windows NT 4 environment and Windows 2000 domains. If appropriate, a test resource domain should also be constructed. One approach to setting up a good lab scenario is to restore production servers from a back-up device in the lab. In addition, bringing up a BDC in the production Windows NT domain and then moving it into the lab and promoting it to a PDC in the lab will allow for a real copy of your production domains users and groups.

The resource domain will need to trust the source master account domains -- creating a two-way trust between each master account domain and the Windows 2000 domain.

Several migration projects could be created to simulate migration of business units. Reports can be run during testing from inside the project (information specific to the migrated objects) and globally for the domain (information about the entire source domain). The DMA product will record results (success and failure) of the test migration projects.

The DMA product provides Project Wizards for migrating users, groups and machine accounts to a Windows 2000 environment. It also supports Enterprise Administrator Territories mapping into Windows 2000 OU or NetIQ Directory and Resource Administrator ActiveViews.

For the Novell NetWare environment, NDS OU and resources will be mapped directly into MS Active Directory. The NetIQ NetWare Migrator is able to recreate the existing NDS hierarchy.

The recommended steps are:

- Test the execution of the migration project.
- Record all issues encountered to address in subsequent trials.
- Test all applications and services in Windows 2000 environment, including Active Directory security and file permissions, Exchange, and custom applications.
- Check that monitoring tools continue to work.
- Create a guideline checklist for the actual migration.

Phase 3: Domain/Users and Server Resource Migration

At this point, you are ready to actually begin the migration of domains and users to servers. The minimum requirements are:

- Existing Windows NT 4.0 environment as described in the pre-migration state.
- New Windows 2000 environment as described in the post-migration.
- Dynamic DNS environment.
- NetIQ Domain Migration Administrator

When executing the Domain Migration Administrator Project, be sure to:

- Backup every server involved in the migration and verify the backups.
- Use the checklist generated in Phase Two of migration for consistency.
- Make use of contingency plans generated in Phase Two.

Phase 4: Desktop/Workstation Migration

The next step is to perform the migration of desktops and workstations.

Migrating workstation accounts to Windows 2000

- Use minimum hardware requirements and compatibility results from Phase One.
- 96 to 128 MB of RAM is often required for optimum performance.
- Confirm that performance on existing hardware will be acceptable.
- Provide Windows 2000 training for your end users as necessary.

Executing Domain Migration Administrator Project

- Backup any important data on workstation and verify the backup.
- Use the checklist generated in Phase Two of migration for consistency.
- Make use contingency plans generated in Phase Two.

Installing Windows 2000 on user Workstations

- A desktop rollout is beyond the scope of workstation migration.
- Workstations can also be upgraded to Windows 2000 preserving the Windows NT 4.0 configurations and settings.

Phase 5: Post-Migration Testing and Cleanup

Upon completing the migration, both the Windows NT 4.0 environment and the Windows 2000 environment will be operational. Users can be gradually moved to the new environment.

After completing the migration using the project plan:

- Re-test everything in the new Windows 2000 environment.
- Confirm that users can login and application servers can be accessed.
- Confirm correctness of AD security functions.
- Move a small subset of users to the new environment as a pilot.
- After a successful pilot, remaining users can be migrated to the Windows 2000 environment.

Common Issues That Effect Migration

There are two common issues that account for a majority of problems encountered during the execution of a migration project:

- Connectivity
- Permissions

Connectivity

Name resolution and connectivity are imperative for a successful migration project testing and execution. The migration dispatcher COM object will request the location of specified resources for installation of the ActiveAgent. If the WINS database has an outdated entry or does not have an entry for the desired resource, the dispatcher cannot copy files and install the ActiveAgent. The migration dispatcher will report any errors due to name resolution or connectivity (rc=53 *The network name could not be found* or rc=67 *The shared resource does not exist*).

Note that WINS must be configured in a Windows 2000 environment with Windows NT 4 clients. In addition, the server service must be running on all systems to be contacted by the dispatcher. The dispatcher will attempt to connect to the Admin$ share (administrative share created by the Server service).

Permissions

In order to install the ActiveAgent component on remote machines, the user account being used to perform the migration must have Administrator authority on the system where the component is to be installed.

Determine if Domain Admins group of source domain is a member of local Administrators group for all machines going to be translated and/or migrated (domain membership change). The migration dispatcher will report any errors due to insufficient permissions (rc=5 Access is denied).

Additional Information to Consider

This section provides additional information about the migration process and related Windows 2000 technologies.

Understanding SID History

SID History allows a user to retain access to resources protected by local groups and ACLs containing the pre-migration source user and group SIDs. In a native mode Windows 2000 domain, user interactive logon creates an access token containing the users primary SID and global group SIDs -- in addition to the user SID History and group SID History values.

The requirements for implementing SID History are:

- Target domain must be Windows 2000 native mode.
- Migration must be run from DC in target domain.
- Source and destination domains must not be in the same forest.

- Source domain must trust the target domain.
- Logged-in user must be a member of Domain Admins global group in target domain.
- Logged-in user must be member of Administrators group on source.
- Auditing must be enabled on target domain (User / Group management events = success and failure)
  - Event ID 718 (success) and 719 (failure) are generated on the target DC when SID History is implemented during the migration process.
- Auditing must be enabled on source domain (User / Group management events = success and failure).
- Domain local group named *NetBIOS*$$$ must exist on the source domain
  - No specific event IDs are generated by the Windows NT 4 source PDC, so the implementation of SID History can be audited by monitoring Local Group Member Add (Event ID 636) and Member Delete (Event ID 637) audit events in the source domain and searching for events referencing the special group name, *NetBIOS*$$$.
- The migration source must be the PDC (in Windows NT 4.0) or PDC emulator (in Windows 2000).
- Source SAM must listen on TCP / IP in addition to named pipes.
  - Create secure channel with registry value on PDC (or emulator):

    ```
    HKLM/System/Current Control Set/Control/LSA – TCPIPClientSupport -
    Reg_DWORD = 1
    ```

  - Reboot the DC for the change to take effect.

The Domain Migration Administrator migration wizard will assess the requirements outlined in blue during configuration. If not present, the operator can choose to configure the options before the migration is executed. The wizard will not assess the credentials of the user executing the migration, the installation location of the DMA product or the trust configuration of the source and target domains.

Security Issues When Using SID History

- If users and his related groups are migrated to the AD using SID History, the group membership of the Windows NT groups migrated becomes static.
  - If the user is then removed from the group in Windows NT the Windows 2000 user account will still have access to data that this group has access to. This is because the SID of the user account has been added to the SID History of the group in Windows 2000 and taking a user out of the group in Windows NT doesn't remove that user account SID from the SID History of the group in Windows 2000. The Windows 2000 group has access to everything that the Windows NT group has access to because of the SID History attribute of the Windows NT group.
- Auditing (File, Registry, etc) is not tracked on accounts (users and groups) that have access to data based on SID History attributes
  - For example, a user account that is migrated to Windows 2000 using SID History and auditing is set up on a directory for his old account. If he then makes changes to data in this directory using his Windows 2000 account, there will be no entries in audit log on the system he is accessing.

- Windows NT tools (Explorer) only show that the source domain accounts have access to resources, even though via SID History Windows 2000 account also have access.
- Windows 2000 tools (Explorer) only show that the target domain account has access to objects (it translates SID History), even though Windows NT 4.0 accounts also have access.
- Once the last PDC is removed from the source domain, accounts from that domain will not be shown with access using Windows NT tools. Then, permissions will show an unknown account or no account permissions will be displayed.

Technical Issues When Using SID History

- SID information for each users and all of the groups they are a member of is added to the target user or group -- increasing the size of the Active Directory
- All SID histories and group memberships can have a total of 1,023 attributes.
- Kerberos authentication packets size issue. (For more information, see TechNet article Q263693).

Partial List of Windows 2000 Technologies

- Messaging (Exchange)
- Remote Access Services (RAS)
- Active Directory Services
- Clustering for High Availability
- Distributed File System
- Windows NT Distributed Security Services, Security Support provider interface
- PPTP and L2TP Private Networks
- Microsoft Transaction Server
- Microsoft Message Queue Server
- Microsoft Certificate Server
- Microsoft Index Server
- Windows NT File System
- Windows NT Directory Services Client Support
- Kerberos Security with x.509 certificate mapping

Migration Checklists

Inter-Forest Migration: Native Mode Windows 2000 Target

Required Configuration Items:

	Task
❑	**1.** Verify that name resolution is functioning: ✓ DNS – required for the Active Directory. Use *nslookup* command line utility to verify name resolution ✓ WINS – required for Windows NT 4 clients and servers
❑	**2.** Verify that domains and systems to be migrated are online and available: ✓ Browse My Network Places for domains and systems to be migrated
❑	**3.** Verify that the source domain trusts the target domain: ✓ This is required for appending the SID History attribute to the target domain account.
❑	**4.** Select account to be used for migration: ✓ Must be an Administrator in the source and target domains. ✓ Must be a member of the Domain Admins group in target. This is required for appending the SID History attribute to the target domain account. ✓ Must have the Permissions Admin role for the Exchange site to be translated.
❑	**5.** Login to Domain Controller of target domain with selected account: ✓ Install NetIQ Domain Migration Administrator on DC of target domain. This is required for appending the SID History attribute to the target domain account.
❑	**6.** Verify Access 2000 is installed: ✓ Access 2000 run-time is included on the DMA installation CD.
❑	**7.** Create MAPI profile for mailbox on Exchange Server in site to be translated.

Optional Configuration Items:

	Task
❑	**1.** Verify that Admin$ share exists on all systems to be migrated: ✓ Created by the server service automatically unless disabled. ✓ Can only be accessed by Administrators.
❑	**2.** Verify that target domain trusts source domain:
❑	**3.** Select account in source domain that is member of Domain Admins group. ✓ This account can be used to change the domain membership of workstations. ✓ Account must be in local Administrators group of every workstation (explicitly or by global group membership).

Inter-Forest Migration: Mixed Mode Windows 2000 or Windows NT 4 Target

Required Configuration Items:

	Task
❑	**1.** Verify that name resolution is functioning: ✓ DNS – required for the Active Directory. Use *nslookup* command line utility to verify name resolution ✓ WINS – required for Windows NT 4 clients and servers
❑	**2.** Verify that domains and systems to be migrated are online and available: ✓ Browse My Network Places for domains and systems to be migrated
❑	**3.** Select account to be used for migration: ✓ Must be an Administrator in the source and target domains. ✓ Must be a member of the Domain Admins group in target. This is required for appending the SID History attribute to the target domain account. ✓ Must have the Permissions Admin role for the Exchange site to be translated.
❑	**4.** Select system to be used for migration console and dispatcher: ✓ Must be Windows 2000 – Server or Professional
❑	**5.** Login to selected machine with selected account: ✓ Install NetIQ Domain Migration Administrator
❑	**6.** Verify Access 2000 is installed: ✓ Access 2000 run-time is included on the DMA installation CD.
❑	**7.** Create MAPI profile for mailbox on Exchange Server in site to be translated.

Optional Configuration Items:

	Task
❑	**1.** Verify that Admin$ share exists on all systems to be migrated: ✓ Created by the server service automatically unless disabled. ✓ Can only be accessed by Administrators.

Intra-Forest Migration: Native Mode Windows 2000 Target

Required Configuration Items:

	Task
❑	**1.** Verify that name resolution is functioning: ✓ DNS – required for the Active Directory. Use *nslookup* command line utility to verify name resolution ✓ WINS – required for Windows NT 4 clients and servers
❑	**2.** Verify that domains and systems to be migrated are online and available: ✓ Browse My Network Places for domains and systems to be migrated
❑	**3.** Select account to be used for migration: ✓ Must be an Administrator in the source and target domains. ✓ Must be a member of the Domain Admins group in target. This is required for appending the SID History attribute to the target domain account and using the MoveObject API. ✓ Must have the Permissions Admin role for the Exchange site to be translated.
❑	**4.** Login to Domain Controller of target domain with selected account: ✓ Install NetIQ Domain Migration Administrator on DC of target domain. This is required for appending the SID History attribute to the target domain account.
❑	**5.** Verify Access 2000 is installed: ✓ Access 2000 run-time is included on the DMA installation CD.
❑	**6.** Create MAPI profile for mailbox on Exchange Server in site to be translated.

Optional Configuration Items:

	Task
❑	**1.** Verify that Admin$ share exists on all systems to be migrated: ✓ Created by the server service automatically unless disabled. ✓ Can only be accessed by Administrators.
❑	**2.** Verify that target domain trusts source domain.
❑	**3.** Select account in source domain that is member of Domain Admins group. ✓ This account can be used to change the domain membership of workstations. ✓ Account must be in local Administrators group of every workstation (explicitly or by global group membership).

NetWare/NDS to Windows 2000/Windows NT 4

Required Configuration Items:

	Task
❑	**1.** Verify that name resolution is functioning: ✓ DNS – required for the Active Directory. Use *nslookup* command line utility to verify name resolution ✓ WINS – required for Windows NT 4 clients and servers
❑	**2.** Ensure Windows 2000 system running the NetIQ NetWare Migrator has the Novell Win32 client version 4.7 or greater: ✓ Should run the NetIQ NetWare Migrator on the Windows 2000 file server if files are being transferred to reduce the number of file copies over the wire.
❑	**3.** Select account to be used for migration: ✓ Must be an Administrator in the target domain and on the target file server. ✓ Must be an Admin (or Supervisor) for the NetWare account.