Economical solutions for migrating file services from Microsoft Windows file servers to HP ProLiant Storage Servers

Introduction

As newer generations of computer hardware and software become available to replace the older, obsolete versions, network administrators are increasingly facing the task of migrating critical data and services from one platform to another. The network administrator must consider several factors to ensure that the data or service being migrated is not compromised in the process and that the process itself does not impact productivity. In small companies, the limited resources and expertise available to plan and execute a migration complicate this task.

This document outlines the primary issues involved and the methods available when migrating file services and associated data from legacy Microsoft® Windows NT® 4.0 and Windows® 2000 File Servers to HP ProLiant Storage Servers. The discussion primarily focuses on migration solutions that apply to relatively simple environments that involve only a few servers and a modest amount of data. These solutions will be of most interest to smaller companies that are interested in simple, inexpensive tools to satisfy their migration needs.

Since these simple tools typically require some manual configuration of the systems to complete the migration, the administrator is assumed to have a fair amount of expertise with Windows in a networked environment. It is also assumed that a certain amount of downtime can be tolerated while the data is moved from one system to another.

For more complicated migrations, or migrations that require almost no downtime or impact on productivity, the customer is encouraged to consider a data migration tool, such as the Quest Consolidator from Quest Software. These tools not only assist in migration planning and execution but also provide storage analysis so that the customer can determine how storage is utilized on the network. For more information, visit http://www.quest.com.

Some customers may be interested in expert guidance in planning and executing a migration. In these cases HP Services offers many comprehensive migration solutions that can be customized and delivered to meet the specific needs of the customer.

Migration issues

Preserving security

When migrating data from one storage system to another, the most important aspect of the migration is ensuring that the security metadata associated with each file and folder remains intact. On a Windows system, security metadata consists of ownership and an Access Control List (ACL) for each file and folder. When a file is copied from one location to another, Windows normally applies new security metadata to the file by inheriting permissions set on the parent folder. A migration mechanism must ensure that every file and folder maintains its original security metadata when it is transferred to its new location.

Preserving attributes and time signatures

In addition to security metadata, files also contain other metadata such as time signatures and attributes such as the archive bit. Standard copy operations normally reset some of these attributes and signatures, such as the Last Modified time signature. When data is migrated, all of these settings must remain unchanged.

Updating clients

In Windows, the "share" is the mechanism by which files and folders are presented to the network for access by client systems. All shares on a server are exclusive to the server where they are created. Client systems access shares by addressing the server name as well as the share name, as follows:

\\servername\sharename

Client systems usually create automatic connections to network shares, such as maps to drive letters. If the share, or the server hosting the share ever goes away, then the client connection to the share will be lost.

When files and folders are migrated, the name of the server (servername) typically changes. This means that all clients that automatically attach to the shares on the server will no longer work. When a migration occurs, the clients must somehow learn of the new server to attach to and make the appropriate adjustments.

In cases where several servers are being consolidated into one, naming conflicts may arise in the naming of shares, as each share name on a given server must be unique. There is also the potential of naming conflicts in the naming of folders and files. All naming conflicts must be resolved during the migration.

Less obvious is the impact made to files and mail messages that contain embedded references to files on a file server. When files are migrated to a new server, all embedded references become invalid. A good migration tool searches out these references on servers and client systems on the network and automatically updates them. Without this automated approach, however, clients must be updated manually.

Minimizing impact

Any migration effort must consider the impact on end users. The productivity of the clients can be affected in many ways. Some of the more common issues are as follows:

Impact to file access

If files are being copied from one location to another, you want the files to be offline during the process to eliminate the possibility that files are being modified during the migration. If files are being copied to the new location, or backed up and restored to a new location, then it is best done during off hours, when the server may be taken offline. Note that this is not an issue for tools that replicate data between systems, as replication software is designed to generate exact copies while systems are online.
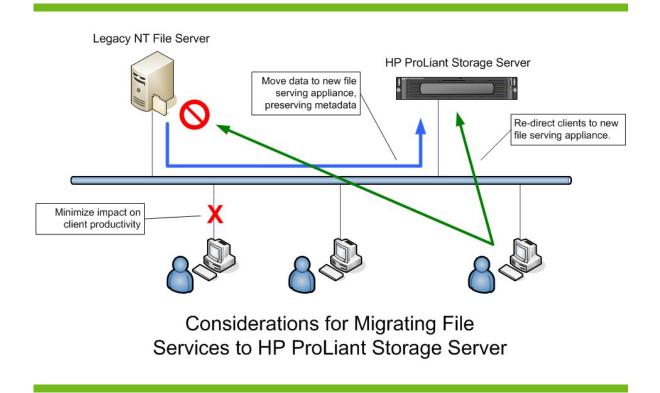
Impact to network bandwidth

If files are migrated online over time using a replication tool or a migration tool, then you must consider the potential impact to network bandwidth. Moving large amounts of data all at once can consume a fair amount of bandwidth and cripple the responsiveness of the network.

Impact to share access

When a cutover is made from one file server to another, share access will be lost to all clients until they are remapped to the new server.

It is important to plan the migration with these issues in mind so that clients are only minimally impacted.

Considerations for Migrating File
Services to HP ProLiant Storage Server

Migration options

There are several methods available to migrate data from one Windows server to another. All of these methods preserve the file metadata intact. The suitability of each method will depend on the particular circumstances of the customer.

1. Copy data directly from one server to another using the XCOPY command. The advantages of this method are that it is free, does not require additional hardware, and is relatively fast. The drawback is that it requires the system to be taken offline while the data is migrated, which could be many hours. Also, XCOPY has some limitations that might prevent some files and some file metadata from getting migrated. The user is encouraged to understand these limitations before proceeding with a migration.

2. Use a qualified backup package to back up the data from the legacy server and restore the data onto the target system. If the customer already has a backup system in place, this may be a good option.

3. Use a qualified data mirroring (replication) package, such as HP OpenView Storage Mirroring, to replicate the data between the two systems. The advantage of this method is that the migration can be performed online. The drawback is that replication packages are usually too expensive to be used as a migration tool. Storage Mirroring is available for free on a 60-day trial basis. A migration using Storage Mirroring may be qualified in advance before licenses are purchased.

4. Use a migration package, such as Quest Consolidator from Quest Software. Such packages provide comprehensive tools and they allow the migration to be planned and executed with virtually zero impact on client productivity. Migration packages usually provide the most value in environments where several servers are involved, there is a considerable amount of data to migrate, downtime cannot be tolerated, or other circumstances exist that would otherwise complicate the migration process.

The first two options will be explained in more detail in this document. These options are the most simple and inexpensive migration methods available to the administrator. They are suitable for environments where only a few servers and a modest amount of data must be migrated. The last two options are suitable for more complex environments. An in-depth discussion of these options is beyond the scope of this document.

Direct file copy method

The XCOPY.EXE program is a standard copy tool installed on all Windows systems. In Windows 2000 and Windows Server 2003, the XCOPY command was enhanced to include a switch that allowed the preservation of file metadata when copied. The program does not support a graphical (Windows) interface. The program must be executed from the command shell. It is designed to copy files and folders to and from NTFS partitions with security intact.

Following are the relevant parameters for using XCOPY to migrate data.

xcopy source destination [/O][/X][/K][/E][/Y][/H][/C]

source	Specifies files to copy
destination	Specifies where to copy files
/O	Copies file ownership and ACL information
/X	Copies file audit information
/K	Copies file attributes
/E	Copies all files in subdirectories
/Y	Suppresses prompting
/H	Copies file with hidden attribute set
/C	Continues copying even when errors are encountered

Do not use this solution to copy files to or from FAT, HPFS, or other non-secured file systems.

The XCOPY command is implemented as part of the Windows Storage Server 2003, which is the core of all HP ProLiant Storage Servers. The customer may migrate data from legacy Windows NT 4.0 and Windows 2000 File Servers to HP ProLiant Storage Servers by running the XCOPY command in a command window on the storage server. Since legacy Windows NT 4.0 servers do not support the /O switch on the XCOPY command, the migration must be executed from the NAS server. Since the XCOPY command is not supported within the web-based management interface of the NAS server, the user must use an alternative mechanism, such as a direct console connection (monitor, keyboard, and mouse), or Microsoft Terminal Services.

Two important caveats to using the XCOPY command to migrate data include:

1. The File Creation date will get updated to the current date and time when the file is moved to the new location. The XCOPY command does not have a mechanism to override this operation.

2. The XCOPY command cannot transfer files where appropriate permissions do not exist. The security mechanisms in Windows allow files to be protected from virtually anyone accessing it, even the administrator. Such files cannot be accessed for copying to a new location using XCOPY. The system will output an "Access Denied" message when attempting to copy files where permissions are insufficient.

The administrator might want to use the /C option when copying so that the operation goes to completion, and then redirect the output to a file so that copy errors can be examined after the fact.

When planning to migrate data using this procedure, it is important to schedule the systems to be offline during the entire copy process. This means that the clients should have no access to the data during that time. This will prevent problems if client systems attempt to change files during the migration process. The administrator should estimate how long the migration will take by measuring how long it takes to move a small amount of data. This will allow the administrator to plan when to perform the migration and how long it should take.

While the XCOPY method of data migration is simple and inexpensive, it might consume many off hours of the administrator's time, as the operation is only suitable for data that is offline.

Tape Backup/Restore method

If the data on a legacy file server is being backed up to tape on a regular basis, then it may be practical to use the tape backup to migrate the data to the HP ProLiant Storage Server. Since HP ProLiant Storage Servers support all the popular backup packages available for Windows, the HP stoage server should support the equivalent backup agents being used on the legacy Windows server. Therefore, a simple restore operation on the storage server will provide a complete and accurate image of the data that was originally on the source.

The image restored to the new HP ProLiant Storage Server should be an exact copy of the original. The Tape Backup/Restore method does not suffer from the caveats of the XCOPY method. Backup applications can back up and restore all files and folders in a file system, regardless of the permission settings on the files (assuming the backup is performed with Backup Operator rights). In addition, backup applications can restore all the time signatures on a file or folder (that is, Creation Date) to their original settings.

The primary drawback of this method is that an investment must be made in a tape backup solution. If the customer already has a solution in place for the existing file serving infrastructure, then this solution may be leveraged to perform the migration. The other drawback to this method is that the servers must be offline while the backup and restore is performed, which may be a long time. This issue may be mitigated through the use of a differential backup and restore.

Following is an outline of how this is accomplished:

1. The old system is backed up to tape following the normal procedure (usually overnight).

2. The next day, the tape is restored to the target file system on the HP ProLiant Storage Server, while the old system is still online and serving files.

3. While the files are being restored on the new system, the old system is still online, and files continue to be modified, created, and deleted. These changes must be accounted for before the cutover to the new system is performed. At the end of the day, the old system is taken offline, and the cutover is executed as follows:

a.　A differential backup is taken of the old system.
　　b.　The changes in the differential backup are restored to the new system.
　　c.　The new system is configured with equivalent shares and share security.
　　d.　The new system is placed online; the old system is retired.

The last step should only take a short time since the backup and restore only involves the changes made in one day. It is important to note that tape backup and restore applications are not specifically designed as migration solutions. Since the tape is being backed up on one system and restored to another, the administrator will want to plan and test the process to ensure it works as expected. Every backup application will exhibit slightly different behavior when differential tapes are restored to different machines. For example, restoring the differential backup may not remove files on the target system that were deleted on the source.

For companies that already have a backup solution in service for the existing file servers, this migration method is just as economical, and will provide a more accurate copy of the data than the XCOPY method. However, the company must still be able to tolerate downtime while the backup, restore, and cutover are performed.

Additional considerations

Beyond migrating data to new storage systems with metadata intact, a number of peripheral details must be considered by the administrator.

1. Be prepared to restore shares and share permissions manually. During migration planning, it is a good idea to record all of the share names and associated paths and permission settings on the legacy systems. After the data is migrated, this information can be used to manually recreate the share environment on the new system.

2. Update clients with new share locations. Since client systems keep track of remote share connections for the convenience of the user (such as an X: drive), these references will become invalid after a migration. The clients must manually delete their existing connections, and reconnect to the new ones. It may be appropriate to announce the changes to the users on the network by e-mail and have them update their own systems themselves.

3. Remember locally defined permission settings on files will become invalid when the files are migrated. In the ACL of a file, several user and group entries with associated access rights are listed. The users and groups in the list might be accounts defined on the local computer, or (more likely) they might be accounts defined in the Domain (or Active Directory). If an ACL contains user or group entries that are local to the computer, then those references become invalid when the file is migrated because the target computer has no knowledge of the local account information that was defined on the source computer. A common practice on Windows NT systems is to set permissions on files with local groups that contain a set of Domain user accounts.

4. If multiple servers are being consolidated, look out for name conflicts in files, folders, and shares. Resolve these conflicts before you begin your migration.

5. Consider that links to migrated files in other files and mail messages are going to be broken. This includes obvious links, such as clickable references made in mail messages, to the not so obvious, such as OLE links embedded in documents, spreadsheets, drawings, and presentations.

The preceding issues should be carefully considered before executing a migration plan. Any one of these issues could cause many hours of extra work or lost productivity if not accounted for in advance. In more complex environments, where these issues become difficult to address manually, data migration tools usually offer built-in features to automatically locate and migrate these elements on a network.

Following are a few techniques that might be helpful in some migration scenarios:

1. In the simplest of cases, where the data from only one server is being migrated to another, the new server could be set up to take the place of the one being replaced. This migration will allow share names to be preserved so that client maps to shares and file links are not affected. The administrator removes the old server from the domain, and inserts the new server in its place. To minimize impact to the clients, all shares on the new system should be identical to the shares of the old system.

2. Microsoft's Distributed File System (DFS) is a feature that allows customers to aggregate file serving resources from multiple systems to be shared and managed from a single location. One of the benefits of DFS is that it provides a level of indirection between the clients and the shares on the remote file system. This level of indirection may be used as a tool to help migrate clients in stages. DFS may be implemented on the target NAS system to redirect users to existing shares on old file servers. This allows clients to be migrated to the DFS shares over time (the old shares and the new DFS shares can co-exist). When all of the clients are using the new DFS references, then the data can be moved to the new server, and the DFS references can be changed to the new server. DFS can also be used on an ongoing basis to provide a level of indirection to file resources so that if they are ever moved, the clients are not affected.

Summary

For simple data migration tasks from Windows NT and Windows 2000 servers, files can be moved to new storage by using the pre-existing backup infrastructure or special copy commands found in Windows Storage Server 2003, as installed on HP ProLiant Storage Servers. These processes are relatively simple, as the data can be taken offline for a period of time. Redirecting clients to the new storage location may be handled manually, assuming that the organization can abide a small amount of interruption.

It is important to note that the suggestions outlined in this document for migrating data from legacy Windows NT File Servers to HP ProLiant Storage Servers are only intended for relatively simple circumstances, and are not intended to be used in larger file serving environments. Where environments are more complex, with several servers, many clients, or a significant amount of data, there is an increased potential for complications and disruption. In such cases, a qualified migration and consolidation tool, such as Quest Consolidator from Quest Software, is highly recommended.

For more information

For additional information on HP ProLiant Storage Server solutions, visit:
www.hp.com/go/storageservers