CommVault Systems White Paper

Giant Step Forward, No Steps Back

Protecting Your Data during Microsoft Windows Migrations

CommVault Systems
Corporate Headquarters
2 Crescent Place
Oceanport, New Jersey 07757-0900 USA
Telephone: 732-870-4000

For more information about CommVault Systems enterprise data management solutions, please phone us or visit our web site at http://www.commvault.com

© Copyright 2003 CommVault Systems, Inc., Oceanport NJ. All Rights Reserved.
All information contained in this document is subject to change without notice.

Giant Step Forward, No Steps Back

Protecting Your Data during Microsoft Windows Migrations

CommVault
Systems

Giant Step Forward, No Steps Back

Protecting Your Data during Microsoft Windows Migrations

Introduction

In many ways, upgrading an operating system or the applications that an enterprise is using is similar to upgrading your car. When looking at new cars, you are often wowed by the countless features available with the new car; however, you may feel safe and secure driving around in your current transportation. Buying a new car gives you options and often reliability that is not found in your current car, but may do so at the expense of money as well as your comfort.

Perhaps your current operating system is like a 1976 Ford Pinto. It may not be the best to look at, it is not the most reliable, and in fact many might even be surprised that it is still running. While everyone at your organization may agree that the time to upgrade or migrate to a new infrastructure has arrived, many likely fear the potential loss or inability to recover older e-mail and versions of files in the event that something in the upgrade fails or the new legal guru comes along and requires something strategic (ranging from financial data to the CxO's MP3 files). Whether you are moving to a Microsoft• Windows 2000 or Windows Server 2003 infrastructure, the availability and recoverability of both data and configuration information such as Access Control Lists (ACLs) should be a primary concern. For example, if an upgrade fails or a request for "pre-upgrade" data occurs, can user access be restored in minutes, hours, or days? This paper discusses many common techniques for migrating data, security principals (users, computers, etc.), and mail servers. It also covers post-migration data availability issues—how will the data that was backed up before the migration be recovered?

Planning for Migration

When planning to migrate data and operating systems from one platform to another, three factors must be considered, which include:

1. What are the organizational requirements of the migration?
2. What are the technical requirements of the migration?
3. Are there any guarantees that the new infrastructure will work?

These factors are discussed below.

Organizational Requirements

Organizational needs drive most decisions to migrate to a new operating. Sometimes the feature and support benefits of a new application or operating system is the driving factor

behind the upgrade. Perhaps customers require fast access to data and the organization wishes to further secure data access. Or maybe, scalability is a key concern. Your current operating system may not be able to evolve with the requirements of newer applications or data storage. As needs change, can the new OS adapt? The need for data availability also drives migration decisions. To ensure uninterrupted data availability, migration to a more robust and reliable OS platform is often the answer.

Technical Requirements

While organizational requirements can justify the business case for an upgrade or migration, technical requirements determine how easy the new operating system will be to manage after the migration, and how smoothly the migration completes. The primary technical requirements for most migrations include:

- Ability to "roll back" migration in case of failure
- Uninterrupted user access
- Uninterrupted application (such as e-mail) availability
- Minimal network administrative overhead

Administrators often worry that once they start down the road to migration, they cannot turn back. This is why having reliable and high performance data protection is so important to the migration process. Prior to beginning a migration, data must be managed and protected so that you have the option of rolling back to the start of the migration process. Since most migrations are incremental in nature, data protection must be available throughout the duration of the migration progress. Finally, once the migration is complete, your data protection solution must continue to protect new data as well as be able to recover data from the older platforms. With these considerations in mind, it is crucial that you have a heterogeneous backup and recovery solution in place that can protect all of your platforms throughout the migration process.

The level of required protection, and simple data and storage management from a single console, can only be found in CommVault Galaxy, which is a key element of the CommVault QiNetix software. The CommVault QiNetix platform, based on CommVault's Common Technology Engine, integrates Galaxy backup and recovery, data migration, data high availability, storage resource and SAN management software solutions. Customers can deploy individual products or seamlessly integrate new elements into an existing CommVault solution, at a fraction of the time, effort and money required by separate point products.

Another key concern with nearly all migrations is user access to data and applications. For many organizations, critical data on file servers must always be available throughout the migration process. This also holds true for critical applications such as Microsoft Exchange. Oftentimes, the most difficult technical challenges of a migration are performed on weekends, so that users do not experience any interruption in service.

One of the more challenging technical goals of any migration deals with application data and access. When upgrading from Exchange 5.5 to Exchange 2000 or Exchange Server 2003, if a failure occurs can you ensure that on Monday morning users will still have access to their original mailboxes? E-mail and Outlook specifics like Contacts, Calendar Items and Tasks are often critical for the smooth flow of business. After all, some users cannot possibly get any work done without e-mail or Internet access! To assist in this problem, CommVault Galaxy gives you the ability to back up Exchange 5.5 mailboxes, and then restore them to any other Exchange 5.5, Exchange 2000, or Exchange Server 2003 system. This way, if a mailbox becomes corrupted during the migration process, all that you need to do is restore the mailbox data from the latest Exchange 5.5 server mailbox backup. With Galaxy, you can even restore individual mail messages, Contacts, or Calendar events if needed.

Finally, if you are moving to new technology, shouldn't it make life easier? If you have additional administrative overhead, such as a requirement to maintain a backup server on an old operating system simply for the sake of recovering data, then you may still find yourself facing many of the old daily problems that were common with the older OS. If migrating is not making life easier and in turn making your enterprise less manageable, then perhaps you should revisit your migration strategy as well as choices for migration and administration tools.

Proceed with Confidence: The Importance of MSA Certification

When you migrate to or upgrade your Windows environment, are their any guarantees that your technology choices will be stringently tested by Microsoft, and fully compatible with Windows and maximize the use of the latest Windows technologies? That is where Microsoft Systems Architecture (MSA) certification comes into the picture. Microsoft defines this architecture as:

> *The Microsoft Systems Architecture (MSA) program develops standardized enterprise-class data center architectures. These architectures are optimized for Microsoft Windows. They are tested to ensure levels of security, reliability, availability, and performance that meets and exceeds the expectations of IT personnel responsible for crucial applications. They offer mission-critical computing infrastructures at Windows economies—the most effective solution to today's enterprise computing needs.*

Simply put, MSA leverages today's elite enterprise solutions and defines a set of enterprise technologies that have been thoroughly tested in all aspects of reliability, performance, scalability, ease-of-use, and Windows-integration. In short, the MSA certification is Microsoft's list of recommended technologies (hardware and software) for enterprise environments. You can learn more about MSA certified technologies at www.microsoft.com/msa.

> **CommVault Galaxy is the only MSA-recommended enterprise-class backup and recovery solution for Windows Data Centers. You can find additional information on this Microsoft tested and recommended solution in their prescriptive architecture kit on TechNet at http://www.microsoft.com/technet/itsolutions/edc/pak/pag/edcpago4.asp.**

Migrating Data

While moving data to a new platform can be a nerve-wracking process that often must occur in a short time window, what if something goes wrong? How can you gain access to data to a time before the migration occurred? That is why having a sound data recovery plan throughout the migration process is so important.

Once you have decided to upgrade or migrate to Windows platforms, you need to move your current data to those platforms, or provide the infrastructure that allows for interoperability during the migration process. In this section, we will examine the data migration issues, both from a network administration perspective and from a backup and recovery perspective. In particular, we will examine the relevant issues in migration data from the following platforms:

- Windows
- NetWare
- UNIX/Linux

Migrating Windows Data

While migrating Windows data, you are often faced with two possibilities:

- Upgrade the current file servers to the new Windows OS
- Move data from the old Windows file server to storage on a new file server

Let's examine the issues that you are faced with in either of these decisions.

Upgrading File Servers

The easiest choice to make when moving to a new operating system is to simply upgrade what you currently have in place. While this is an option, it is not always the most logical choice. Many administrators prefer to work with clean Windows installations as opposed to upgraded versions, which is usually due to the history of instability that has plagued upgrades in previous Windows versions. Also, when a file server's operating system is old, odds are that its hardware is outdated too. The decision to upgrade often yields some funding for hardware updates, and you may be able to use the justification for the upgrade to replace outdated and slow-performing server hardware. With these factors in mind, whenever possible it is usually best to move file server data to a new host server.

Moving Data to a New File Server

Sometimes moving data can be as easy as physically moving a disk array and attaching it to a new host system. When this occurs, you can often move data and retain its current access control lists (ACLs). Also, the first time that a moved NT 4.0 (NTFS 4) volume is mounted by a Windows 2000 or higher OS, the volume will be upgraded to NTFS 5, which allows you to take advantage of newer storage and security features, such as Encrypting File System (EFS).

If your upgrade, migration, or restructure involves the movement of data from one file server to another then you will have much more to consider. The technical challenges to overcome during the migration process include:

- How are the ACLs managed?
- What is the impact on the network and server infrastructure during the data movement process?
- How are users impacted during the data movement process?

One of the most efficient ways to move data during the migration process is by using backup and recovery. Consider the illustration shown in Figure 1.

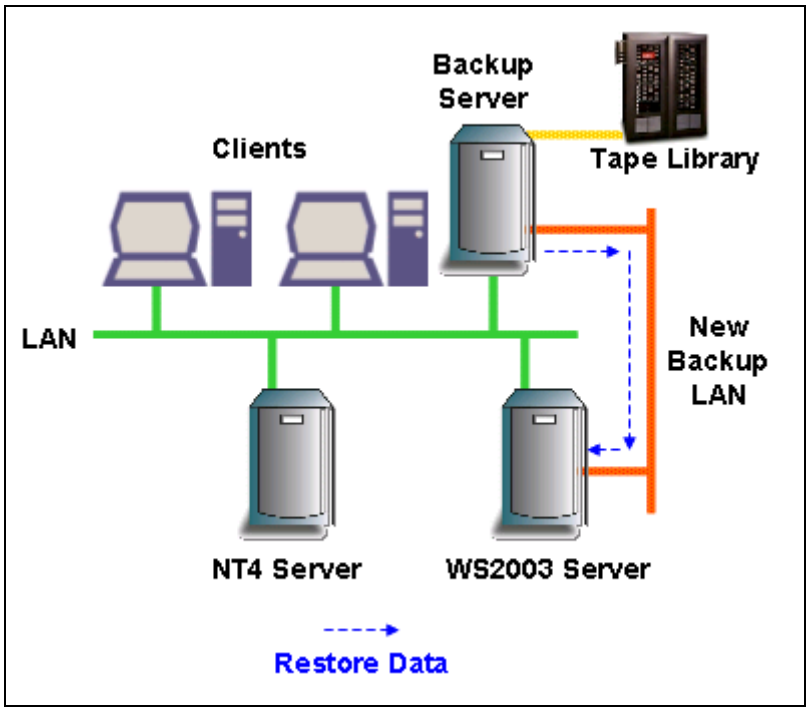

Figure 1: Restoring NT 4 Backup Data to a Windows Server 2003 System

In this example, a new "Backup LAN" is implemented to isolate backup and recovery data from the production network. While this solution requires placing two network interface cards (NICs) in production file servers, it allows you to move data without impacting LAN performance.

With CommVault QiNetix (and Galaxy's) robust media management capabilities, you can use high performance ATA devices, RAID and other magnetic disk devices (as well as tape) as your backup target. Depending on data access needs, the appropriate storage device can be assigned for each data type.

Organizations looking for even higher backup and recovery performance often choose to configure a Storage Area Network (SAN) for backup and recovery data, which offers faster data transfer (2Gbps or higher) than traditional 100Mb Ethernet LANs.

With the example in Figure 1, data can be backed up (if it has not been already) from the NT4 Server and restored to the Windows Server 2003 server. This approach allows you to migrate and test the data while keeping the existing file server online during the migration process. With this technique, users are not affected by the data migration process. Once you are satisfied with the results of the data migration, you can inform users to connect to the new server. CommVault Galaxy greatly simplifies this process. It allows you to back up data on one Windows platform and restore it to another, so you could back up of several file shares on an NT 4.0 server, for example, and restore them to a Windows 2000 or Windows Server 2003 file server.

While moving data either via backup or even a simple "copy and paste" can get the data to a new server, you still must consider the impact on Access Control Lists. By default, moved data inherits the ACLs of its parent. So data that is moved from one file server to another will inherit the permissions that are configured on the target file server.

As an alternative approach to moving data when you wish to ensure that ACLs are maintained, you should determine if your backup software supports the restoring of ACLs. This way, you can simply restore data from the old server to the new server and maintain the existing ACLs.

If you are not migrating domain security principals (users, groups, etc.), then you will need to manually recreate the ACLs on the new system.

After performing the move, you should leave both servers online to verify that all users can successfully access data on the new server. If a problem is encountered, you can direct users back to the older server until you can correct the fault.

With CommVault Galaxy, you can back up files and folders on one system (Windows, UNIX & Linux) and restore them to another system. CommVault Galaxy also gives you the ability to restore ACL's and SID's when older Windows data is restored to newer versions of Windows. Galaxy can also restore a folder tree and its associated ACLs.

Now that we have looked at the Windows migration concerns, let's look at the more difficult data migration scenarios – migrating NetWare and UNIX data.

Migrating NetWare, UNIX and Linux Data to Windows

While migrating or upgrading Windows environments does offer a unique set of challenges, much more must be overcome when you are migrating NetWare, UNIX or Linux servers to Windows. These operating systems are examined in the next two sections.

Migrating NetWare Data to Windows

NetWare migration offers a host of challenges to administrators. To begin, a NetWare migration typically entails moving to a new directory service. This requires moving from Novell Directory Service (NDS) to Windows Active Directory. Moving a directory service structure can be a very cumbersome task. To ease in the transition, Microsoft provides several tools to maintain data access while moving data to Windows servers. The following Windows tools are extremely valuable in the migration process:

- Client and Gateway Services for NetWare (CSNW/GSNW)
- Microsoft Directory Synchronization Service (MSDSS)
- File Migration Utility (FMU)

Let's quickly examine the role of each of these tools in the NetWare migration process.

Client and Gateway Services for NetWare

CSNW and GSNW allow Windows systems to use the IPX/SPX (NWLink) protocol to communicate with NetWare servers. Client Services for NetWare (CSNW) allows a Microsoft system to logon to a NetWare server, while GSNW allows a Microsoft server to act as a gateway to a NetWare server. Organizations use GSNW so that they do not have to install CSNW or the NetWare client software on every one of the Windows clients. Instead, Windows clients can connect to a Windows Server using TCP/IP. If the Windows Server is running GSNW, Windows clients will see shares that actually reside on a NetWare server as appearing to be on the Windows server.

Microsoft has long envisioned GSNW as a way to ease in the migration to what will become a complete Microsoft network. Once client systems have been upgraded to become native Microsoft clients in an Active Directory forest, they can still access a NetWare server's resources through a Windows server running the GSNW service. This provides you with the flexibility to slowly migrate NetWare server data to Windows.

> **If your backup and recovery software supports backing up data via universal naming convention (UNC) paths, then you could back up NetWare server data through a Windows server running GSNW. In turn, this data could be restored to a different Windows server.**

Microsoft Directory Synchronization Service

MSDSS is Microsoft's native tool that gives you the ability to synchronize the directory information that is stored in the NDS with Active Directory. This service gives you the ability to manage accounts from either directory and thus gradually transition your complete environment to Windows Active Directory, if desired. To prevent accidental data loss during the initial directory synchronization, you should ensure that you have a reliable backup of both the NDS and Active Directory database.

> **For Active Directory running on Windows 2000, CommVault supports attribute-level backup and recovery. For Active Directory running on Windows 2003, attribute and object-level backup and recovery are supported. CommVault also supports object-level management within the NDS schema, via a similar LDAP interface.**

File Migration Utility

Microsoft's File Migration Utility (FMU) tool allows you to migrate data stored on NetWare servers to Windows servers, without losing any security information. This is because the FMU integrates with MSDSS. With a properly synchronized NDS and Active Directory, files can be moved from NetWare servers to Windows servers and retain their original ACLs, thus provided for a seamless transition from one operating system to another. As with the directory services, you should ensure that you have a valid backup of your NetWare server data prior to attempting to move any files. This process is significantly streamlined if your backup software supports file-level backup and recovery. This way, if a single file was corrupted during the movement process, you will not have to restore an entire volume in order to get it back.

> **For more information on migrating data from NetWare to Windows, search Microsoft TechNet at www.microsoft.com/technet using the keywords "NetWare to Windows 2000 Server Migration Planning Guide."**

As you can see, Microsoft has taken great efforts to create tools to help you migrate users and computers to a Windows-centric Active Directory infrastructure. Since Windows operating systems are now seen as proven in the enterprise, Microsoft has turned to develop and improve tools to aid in UNIX or Linux migrations.

Migrating UNIX and Linux Data to Windows

In order to help facilitate UNIX/Linux to Windows migrations, Microsoft has a single suite of tools, Windows Services for UNIX 3.0, that can ease the transition of data to Windows platforms. In particular, Windows Services for UNIX 3.0 offers the following benefits:

- *Network File System (NFS) client, server, and gateway services* – Allows you to integrate UNIX and Windows file shares during the migration process.
- *Integrated UNIX utilities* – Allows you to run existing UNIX shell scripts on Windows platforms.
- *Password synchronization* – Provides means for two-way password synchronization between UNIX and Windows servers.
- *Microsoft Interix integration* – Provides for a UNIX environment that runs on top of the Windows kernel, which allows UNIX applications and scripts to run alongside Microsoft applications on Windows servers.

As you can see, several tools are available that help you either migrate from or integrate with UNIX and Linux servers. The key to maintaining availability while moving data across platforms is to have a reliable backup that supports file or directory level restores. This way, if corruption occurs as data is moved from one server to another, you can quickly recover what is needed. Again, since it is essential to manage and protect data throughout the

migration process, you must ensure that you have a solution that can protect your data across the enterprise from beginning to end. With support for the predominant UNIX and Linux operating systems and applications, CommVault Galaxy provides the data management and protection you need during and after any enterprise-scale migration. For more information on UNIX to Microsoft migration, point your web browser to www.microsoft.com/windows2000/migrate/unix.

> **In UNIX and Linux migration and server consolidation scenarios, CommVault can assist dramatically. All UNIX and Linux data that has been backed up by CommVault can be restored directly to Windows.**

Migrating Security Principals

So far, you have already seen that you can migrate NetWare security principals to Windows using MSDSS. For Microsoft domain migrations and restructures, several tools can aid in the migration process. A brief description of each tool follows:

- *Active Directory Migration Tool (ADMT)* – "Jack of all trades" GUI tool that allows you to copy or move objects to a new forest or to move Active Directory objects within the same forest.
- *Clone Principal* – Series of scripts that allow you to copy objects from one domain to a new domain in a separate forest.
- *Movetree* – Command line tool that is used to move users, groups, or organizational units (OUs) to a new location within the same Active Directory forest.
- *Netdom* – Command line tool that is used for migrating computer objects or trusts between domains.

As you can see, Microsoft provides you with many tools for moving and cloning Active Directory objects. Prior to any migration operation involving the Active Directory, you should ensure that you have a valid backup of the System State on at least one domain controller in both the source and target domains. This will allow you to recover any data that may have been lost as the result of a failed migration operation.

> **In addition to backing up the entire Active Directory database as part of the System State, CommVault Galaxy can backup and recover individual Active Directory objects and their attributes on Windows Server 2003 domain controllers, and individual Active Directory attributes for Windows 2000.This is extremely beneficial if an object is lost or corrupted during the migration, as you can simply restore the lost object as opposed to restoring the complete System State on a domain controller.**

Migrating Exchange Mailboxes

When the time arrives to upgrade to Exchange 2000 or Exchange Server 2003, you will be faced with several options. Typically, administrators add the new Exchange server to the domain and use the Active Directory Connector (ADC) so that the Exchange 5.5 server is synchronized with the Windows 2000 or higher domain controllers. With the connector in place, mailboxes can be moved by using Exchange Administrator and selecting the *Tools – Move Mailbox* option. Most Microsoft documentation recommends that you move anywhere from 20 to 30 mailboxes at a time, until the migration completes.

Microsoft documentation also recommends that you use the Exmerge tool to back up individual Exchange mailboxes to .pst files in order to recover mailbox data in the event of migration failure. While this is an option, it is by far the least efficient. Prior to migrating Exchange mailboxes, it is best to intelligently back up the Exchange databases at both the database and mailbox level. Backup applications that support Single Instance message-level and/or mailbox-level backup are best suited for these types of operations. For example, if corruption occurred to part or all of one mailbox during the migration, it can be extremely cumbersome to restore the entire private information store to an older version of Windows, outside of your network. For example, this could easily equate to several hundred gigabytes of data. Instead, if your backup and recovery software has the ability to restore a single mailbox, folder or message to either the source or destination server, a small amount of the corruption in the migration process will result in lost hours or days (or even weeks!).

Remember that Exchange stores much more than just email. Users' Contacts and Calendars are often crucial for day-to-day organizational operations. Being able to secure this data prior to the migration is crucial. Having the ability to simply restore a user's contacts, for example, as opposed to having to a restore an Exchange database to recover contact information will ensure that critical data can be quickly recovered within minutes, if needed during the migration process.

> **To save on Exchange message-level backup data storage space, you should ensure that your backup solution supports single-instance storage of messages and attachments. Most backup solutions only support brick-level backup--this means that a 1MB attachment sent to 10,000 users would consume 10GB of backup media. With true single-instance storage, the attachment would only consume 1MB of storage. CommVault Galaxy backups offer true single-instance storage of all like mail messages and message attachments. Galaxy has unsurpassed granular recovery, down to the mail message and attachments, with all properties intact.**

As you can see, as with moving file server data, it is also important to protect database data such as Exchange mailboxes during any migration. Having a tested backup and recovery plan in place prior to the migration will ensure that if a failure occurs, you can quickly recover.

Post Migration Backup Data Availability

So now that you have completed the migration and ensured that your backups gave you a level of insurance against failure, you now must manage the new environment. Perhaps your migration may evolve over several months or even years. If you are in this predicament, consider the added stress of having to manage backup data with point-level solutions that are geared to support only a single operating system. With the right backup and recovery product, like CommVault Galaxy, you can manage all backup data from a single console.

Aside from numerous management consoles, other backup software products require you to be aware of the physical location of data in order to restore it. This usually equates to having to know the system name and possibly even the backup tape in order to do a restore. What if a system name changes? Your restore plan can then quickly begin to look like a page of "connect the dots" that was attempted to be solved by a three year old. Most legacy backup applications are storage centric, meaning that if you don't know where the data is, you can't get it. Trying to manage data locations as networks evolve over years can be difficult if not impossible, and may even require several full time employees to manage.

The wave of the future is policy-based data management. Policy-based management allows you to manage data backup and recovery transparent to the data's physical location. You just pick what to restore and the backup software will figure out the rest. If you are considering moving your network operating systems out of the Stone Age, you should strongly consider doing the same with your backup software. If your data is taking a step forward, don't leave your data management and protection behind. Today, there is only one solution that can logically manage your data across the enterprise from a single console, giving you the ability to manage and protect legacy data while scaling to the future. Only CommVault Galaxy's data management and protection gives you the assurance you need to know that data will be available when and where it's needed, all the way through your migration. With CommVault Galaxy (and the QiNetix platform), your networks are freed so you can continue taking giant steps forward without ever taking a step back.