Simple Disaster Recovery of FileNet on Windows®: Image Services Using SnapMirror® Technology

Gangoor Sridhara, Network Appliance, Inc.

TR-3424

Abstract

Today, global enterprises need to protect and quickly recover data in the event of natural or man-made disasters, operator errors, or technology and application failures. They also need an efficient way to distribute data to remote locations. Without an effective data protection and distribution strategy, operations can be brought to a standstill, resulting in millions of dollars of lost revenue. As demand grows over time, it must also address scalability and performance issues. Fixed objects may include images, documents, and rich media content. Using SnapMirror technology, a simple yet an elegant solution may be provided to replicate FileNet data from a production environment to a remote location.

Table of Contents

1. General Issues

1.1 Windows

Local file systems versus shared file systems. There are two file system paradigms of interest for FileNet deployment. Modern Windows platforms offer two paradigms for file system deployment: local file systems (NTFS) and shared file systems (CIFS). These options are also referred to as a storage area network, or SAN (local file system), or network-attached storage, or NAS (shared file system). Commercially these paradigms lead to very different storage subsystem products with different costs, capabilities, and scalability. Conceptually, they have only a couple of differences.

Local file systems. This paper will discuss the use of NTFS as the local file system. The local file system interacts with locally attached devices. More recently, Fibre Channel Protocol (FCP) attached devices and SAN devices have come into prominence. The FCP devices are treated as local SCSI devices, but are accessed across a storage network using FCP. The Internet Protocol (IP) based Small Computer System Interface (iSCSI) protocol uses an existing network infrastructure to provide the same benefits of SAN configuration and to configure the storage as the local file system. In this paper, the local file system uses the iSCSI protocol using a regular network infrastructure to configure the local file system on a Windows platform. A database server, FileNet Image Services (IS) and MKF/Cache are recommended to use the local file system. In this paper the local file system is referred to as a SAN or IP SAN configuration.

Shared file systems. Shared file systems allow more efficient use of storage resources by enabling multiple hosts to access data while keeping the data management responsibilities (and costs) off the host system. CIFS scales to multiple hosts in a simple fashion that introduces some additional CPU overhead to process the data through the network stack. The CIFS file system provides flexibility and increased storage efficiency for FileNet environments to use magnetic storage and retrieval (MSAR) surface libraries and SnapLock® storage and retrieval (SSAR) configurations. A shared file system is not recommended for configuring either the database server or the Image services. This paper refers to the shared file system as NAS or the CIFS protocol on Windows.

1.2. FileNet

1.2.1. Overview

FileNet has a range of products that provide business solutions for document and content management needs. The most common and best known of these is FileNet IS. Optical storage and retrieval (OSAR) was once the preferred (and only) storage media choice for image services technology, but technical improvements led FileNet to consider the advantages of magnetic disk media over optical storage. FileNet IS now supports magnetic disk media using its Magnetic Storage and Retrieval (MSAR) software.

It is very important to implement a strategy to replicate this business-critical FileNet Image IS data to a second location. Such a plan will give an advantage to quickly and efficiently bring the server up and running on short notice.

There are several options to replicate the data from the source to a destination site. Some of these options include:

Multi-Synchronous System (MSS) solution offered by FileNet

Multi-Synchronous Committal (MSC) solution offered by FileNet

SnapMirror solution offered by Network Appliance to efficiently replicate the data to a different location

NetApp SnapMirror software delivers the disaster recovery and data distribution solution that today's global enterprises need. By replicating data at high speeds over a LAN or a WAN, SnapMirror software provides the highest possible data availability and fastest recovery for mission-critical applications. The advantages of using SnapMirror include:

Fast data replication and failover. Minimizes downtime costs in case of a failure at the primary site.

Access to mirrored data. Enables offloading tape backup, doubling the value of your disaster recovery investment.

Volume or qtree replication. Mirrors selected data sets, dramatically reducing networking infrastructure requirements.

Replication synchronicity level. One product to control frequency of replication (async, sync, and semi-sync).

More efficient network utilization. Cuts the costs of data replication and disaster recovery.

Easy setup. Needs virtually no added IT resources; allows frequent testing of the disaster recovery plan.

1.2.2. Purpose and Scope

This paper describes the steps necessary to integrate FileNet IS with Network Appliance™ storage devices and replicate the data using SnapMirror technology. It is recommended that readers read the technical report "Integrating FileNet Image Services with Network Appliance Storage Devices," which contains details about Windows platforms, before reading this technical paper. The paper describes a method to implement SnapMirror technology to replicate data.

Note: This information should be taken only as a starting point. Customers should consult FileNet and NetApp Professional Services to determine the configurations most appropriate for their environments.

1.2.3. Introduction

Integration of FileNet IS and a Network Appliance storage solution provides an effective solution for content management. This section describes briefly different components involved in the configuration.

FileNet deployments vary depending on the specific deployment and operating system (OS) platform. CIFS deployments have several important characteristics and either a single host or a multiple host configuration. This section outlines each of these characteristics.

FileNet IS. In order to successfully deploy FileNet IS, a supported relational database server (RDBMS) has to be installed and configured on the necessary storage systems. FileNet software must be installed on the local file system (SAN or IP SAN).

Relational database server (RDBMS). Before installing and configuring FileNet IS, a site-controlled database server must be installed. Several technical reports are available on our external Web site's technical library section.

MKF/cache. Using the local file system to configure the FileNet Multi-Keyed File (MKF) is recommended. Local file system terms refer to storage configured using a SAN or IP SAN network.

MSAR (magnetic storage and retrieval) storage library may be configured to use either NAS or a SAN.

SSAR (SnapLock storage and archival) must use NAS. SnapLock is currently supported only on a shared storage configuration. This is not a drawback as the individual file will be locked down as read-only once the content is populated and ready to be archived for compliance or other purposes.

1.2.4. FileNet Image Services

FileNet enterprise content management (ECM) solutions allow customers to build and sustain competitive advantage by managing content throughout their organizations, automating and streamlining their business processes. It provides the full spectrum of connectivity needed to simplify their critical content management and everyday decision making. FileNet ECM solutions deliver a comprehensive set of capabilities that integrate with existing information systems to provide cost-effective solutions that solve real-world business problems. Image Server delivers faster access to large numbers (billions) of fixed objects such as documents, reports, print streams, faxes, e-mail, and multimedia content. FileNet IS software provides the ability to:

- Improve the operational effectiveness of content information
- Allow high availability yet ensure the security of information assets
- Improve the content access experience of the customers
- Maintain access while preventing data corruption and ensuring security

With FileNet IS software, customer can create a high-performance repository with failover capability and high availability of data while providing effective security. Currently FileNet IS software is supported on Windows, Sun™ Solaris™, HP/UX, and AIX platforms.

1.2.5. Site-Controlled RDBMS

The FileNet IS server supports various RDBMS servers. They include Microsoft® SQL Server, Oracle®, and IBM DB2 servers. For a support matrix, refer to the FileNet Customer Support Website. Our test setup used SQL Server 2000 on a Windows platform. Refer to Oracle or DB2 related technical reports to know more about database replication on our technical library section.

1.2.5.1. Microsoft SQL Server

In order to configure and use SQL Server on a Windows platform, it is recommended that NetApp storage be configured to be used as local disks. This paper recommends using a SAN with an FCP configuration. Existing infrastructure may also be used to configure the local disk storage by using iSCSI. Our test setup used iSCSI to configure the Ethernet-based storage as local storage on the Windows server. Using NetApp SnapDrive™ storage management software is recommended for efficient storage management.

1.2.5.2 Oracle Server

FileNet IS supports various database servers, including Oracle RDBMS servers. For NetApp storage to be used as local storage to the Windows server, configure the storage as local disks. Refer to several Oracle technical papers available for integrating with NetApp storage solutions.

1.2.6. Network Connectivity

A SAN on an existing network infrastructure using iSCSI is known as an iSAN configuration. Both SAN and iSAN configurations provide local SCSI disks to the Windows operating system. FC host bus adapters (HBAs) come with a dedicated 2Gbps Fibre Channel link. Usually FC SAN configurations have a failover server, NetApp storage server, and multipath access to address any single point of failure. If the SnapLock connector for IS software is planned, network connectivity must be CIFS on a Windows platform or NFS on a UNIX® platform. Either the network-mapped drive or the Universal Network Connectivity (UNC) path is supported with SnapLock.

Figure 1 shows a simple single-path point-to-point configuration. Both the Gigabit Ethernet and FC connections are made without using a switch. However, for mission-critical projects it's best to configure the full SAN configuration to address any single point of failure.

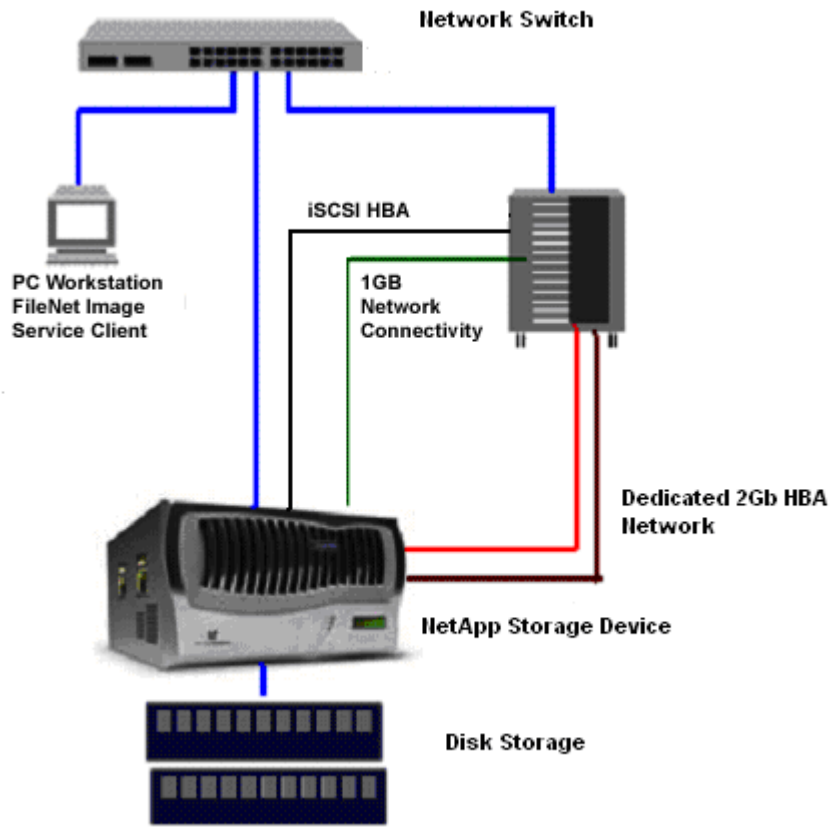

Figure 1) Network connections.

Both the database and FileNet IS software must be installed on the locally configured SCSI disks or on the local disks. For this purpose, our test setup used Microsoft iSCSI and SnapDrive software on a Windows server to configure the LUNs and local disks. FileNet IS can also be configured using FC SAN. In addition, the clustered failover option (CFO) provides higher data availability in an enterprise-level configuration by

eliminating a single point of failure for the storage system. For a FileNet IS configuration, CFO configuration is optional.

1.3 SnapDrive

Network Appliance (NetApp) storage systems are designed to participate in a wide range of operating system environments that may include Windows, UNIX, or Linux®. The storage system also can serve up data as a CIFS/NFS file server or participate in an FCP SAN or iSCSI SAN.

This paper will concentrate on a Windows environment and the access methods that are supported by the NetApp storage systems and Windows.

1.3.1 SnapDrive for Windows

SnapDrive for Windows is a NetApp product that simplifies and automates some of the more difficult tasks associated with using FCP in a Windows environment. SnapDrive installs as a snap-in to the Microsoft Management Console. All management interactions with NetApp storage system LUNs attached to your Windows server must be performed through SnapDrive.

The tasks associated with managing LUNs on the NetApp storage system, such as creating or deleting LUNs or creating or deleting Snapshot™ copies of storage system volumes that contain LUNs, are performed from the SnapDrive interface. There is also an option of using a command-line interface to automate SnapDrive commands directed to NetApp storage system volumes that hold LUNs.

For more information on SnapDrive, please see the NetApp technical report "Technical Overview of SnapDrive™ 2.0," at http://www.netapp.com/library/tr/3197.pdf. For information on installing SnapDrive on your system, please refer to the documentation that comes with the Windows attachment kit, which is either shipped with the storage system or ordered as a separate product.

1.3.2 NetApp Storage System for FCP/iSCSI LUNs

NetApp storage systems support multiple protocols, including FCP, iSCSI, and CIFS. These protocols can be enabled by entering the appropriate license keys. FCP/iSCSI LUNs that are built on a NetApp storage system are special files created on NetApp storage system volumes that can be accessed as local storage on the Windows server. The LUNs are formatted as NTFS drives. This document refers to such storage as local storage system. This paper refers to LUNs created using iSCSI. The procedure to create LUNs using FCP is similar, and more details are available on NOW™ (NetApp on the Web).

1.3.3. CIFS Support

CIFS support is automatically shipped with a NetApp storage system and enabled with a license code. The NetApp storage system can be configured in multiple ways such as CIFS-only files, UNIX only, or mixed. If the storage system is configured as CIFS only, only Windows operating systems can access the storage system resources. Mixed mode allows both UNIX and Windows systems to access the storage system. In our test setup, the NetApp storage system was configured as mixed-mode security that allowed access from both UNIX and Windows hosts.

2. NetApp Storage System Configuration

When running a FileNet server whose data and installation path reside on a NetApp storage system, three areas can affect FileNet server performance: the NetApp storage system, the network connectivity and the operating system (Windows) environment.

2.1 The NetApp Storage System

The NetApp storage system can be configured to optimize FileNet workload performance. Because NetApp storage system supports multiprotocol use, the storage system may be configured optimally to use a local file system and network shared file system.

2.1.1. NetApp Storage System Considerations

Efficient volume and RAID definitions. Volumes defined with too few disks will have lower performance than volumes with larger numbers of disks. The higher the number of disks in a volume, the better the performance will be. The data will be spread across more physical accesses, allowing better parallelism during reads. RAID groups with a small ratio of data disks to the parity disk will make less data storage available, but the chance of double disk failure will be lower. Conversely, a high ratio of data disks to the parity disk will make more data storage available, but the chance of double disk failure will be higher. The new RAID-DP™ storage system volume option can mitigate the double disk failure issue. It is up to the owner of the data to determine the balance between safety and disk economy.

With the advent of Data ONTAP® 7G, efficient volume sizing is now an unneeded exercise. A new storage object called an aggregate abstracts the physical nature of a traditional volume and allows volumes of any size to be defined in an aggregate with many disks. The data residing on this new volume type, called a flexible volume or FlexVol™ volume, is spread across all of the disks that compose the aggregate. A FlexVol volume can be configured from 20MB to 16TB and can share all of the spindles in the aggregate.

Network connectivity. Using a dual-port FCP or hardware-based iSCSI HBA configuration to set up the local file system is recommended. For a shared storage system, a faster network such as a gigabit network path is required.

2.1.2. FCP/iSCSI LUNs Considerations

Enabling space reservation. Enabling space reservation makes creating a backup copy easier. the automatic Snapshot feature must be turned off. The `space_reservations` parameter can be set from the MMC SnapDrive window during LUN creation, or it can be set using the following command:

```
netapp> lun set reservation lun_path disable
```

Snapshot copies can be turned off using the following command:

```
netapp> vol options <vol> nosnap on
```

Group user data on separate storage system volumes. User data sets usually require backups and high availability. Turn Snapshot copies on to ensure that the data can be recovered. Turn space_reservations on to ensure that there will be enough space on the storage system volume to hold the entire allocated data set. Space_reservations is normally set to off. To set space_reservations on, use the following command:

```
netapp> lun set reservation lun_path enable
```

2.1.3. Network Considerations

Gigabit Ethernet connections. Gigabit Ethernet connections will obviously provide better throughput than 10/100 Ethernet connections.

Jumbo frames. Set jumbo frames on if possible. Be aware that jumbo frames are not standardized and can be different sizes to different vendors. Make sure that all participating hardware, including switches, in your network has jumbo frames specified the same.

XMIT/RECV buffer size. The XMIT and RECV buffer sizes should match between the storage system and the Windows client. A multiple of 4K will also align the buffers to the normal storage system unit of work.

2.2 Windows

Several Windows changes can be made to help the NetApp storage system perform better. These modifications generally affect the I/O subsystem and the hardware that supports it.

Use only FCP HBAs approved by NetApp. NetApp will certify those FCP HBAs that have been tested and found to work properly on NetApp storage systems. Use of noncertified FCP HBAs may generate unpredictable results.

Use only FCP switches approved by NetApp. NetApp will certify those FCP switches that have been tested and found to work properly on NetApp storage systems. Use of noncertified FCP switches may generate unpredictable results.

Make sure that Windows is optimized for proper network throughput. From the Control Panel, open Network Connections. Right-click Local Area Connection and click Properties. In "Components checked are used by this connection," double-click File and Printer Sharing for Microsoft Networks. Under Optimization, notice that "Maximize data throughput for file sharing" is selected by default. Turn the option off to reduce paging activity. This can improve network performance quite a bit.

Network interface card parameters. Many network interface cards (NICs) support various performance tuning options. Setting these can improve overall performance. The Intel® Pro Ethernet card is one of the better cards to use. On this card, set Adaptive Performance tuning to "maximum bandwidth."

Increase buffer size. Increasing coalesce buffers, receive buffers, and transmit control blocks from default values can improve performance under certain conditions. DO NOT change these if the Windows 2000 machine does not have a large amount of memory. Remember that changing these options requires a restart. Consult the Help menu on the Intel Pro set config menu for more details.

Window size setting. Large window size basically increases the number of messages that can be in flight. The maximum window size that is supported on a NetApp storage system is 64240. Increasing this on both the storage system and Windows machine can dramatically improve performance for large transfers. You need to set the `cifs.tcp_window_size option` to 64240 on the storage system.

Volume mountpoints. Allow for dynamic data storage growth.

Striped volumes. Multiple storage system LUNs defined on different volumes can be combined to form a logical volume with many accesses. LUNs can also be defined on volumes that reside on different storage system heads for addition throughput.

Network definitions. Network definitions should match the other elements of the network servicing the Windows machine.

Jumbo frames. Jumbo frames should be enabled if possible, and the size should match the other elements of the network servicing the Windows machine. Jumbo frames are not supported on SnapDrive 2.1. However, jumbo frames are supported with CIFS functions over Gigabit Ethernet.

Transmit and receive buffers. The transmit and receive buffers should match the other elements of the network servicing the Windows machine.

3. Assumptions

The reader is assumed to be familiar with the operation of Network Appliance storage devices and the concepts of a SAN and NAS. The reader is also assumed to have a system administrator's knowledge of the FileNet IS server software. The term storage system refers interchangeably to the NetApp storage system or NetApp FAS server storage devices, with the caveat that not all NetApp storage devices support the FC SAN protocol options. The reader is assumed to have FileNet IS-related expertise. It is prerequired that the reader read another technical report that discusses integrating FileNet IS on the Windows platform.

3.1. Infrastructure

A sample system configuration was selected to install and test the product to validate the information in this document. The purpose was to show the procedure for integrating FileNet IS software with a NetApp storage device. Performance specifications and tuning are not within the scope of this document.

A similar type of infrastructure was used on both primary and destination locations. It is not required that both locations have exactly the same type of hardware infrastructure to replicate the data. However, care must be taken to ensure the support matrix in order to successfully replicate the data. The simple configuration required to run the Microsoft SQL Server 2000 database with FileNet IS 4.0 on a Windows 2000 host with a storage system is listed below:

- FileNet IS 4.0 on a Windows 2000 server
- NetApp storage system with CIFS, iSCSI, and FCP capability
- Network for management and data flow
- FileNet IS-required environment settings such as user accounts, software, storage appliance mountpoints, and/or SAN storage

In this document, the following infrastructure is used for completing the installation of IS software:

NetApp storage system command prompt `boy> sunday>`

The Windows host name at primary site `butthead`

The Windows host name at remote location `beavis`

Operating system users `'fnsw' 'oracle' 'root'`

Command output is in courier font.

Using the SnapDrive tool, it is easy to configure and manage the storage system. On our test setup, we used three LUNs to map them to a LUN group and completed the local disk configuration. Figure 2 shows the disks configured under the Storage section using SnapDrive software on the remote site. This setup is similar to that of the primary site system.

The following infrastructure was used to set up a FileNet environment over Ethernet using Windows CIFS to files stored on a NetApp storage system:

- Workstation based on Intel running Windows 2000 and FileNet software
- Network Appliance storage system licensed for CIFS and iSCSI
- IP-based Ethernet network

SnapDrive software

An IP-based Ethernet network is required for the host to communicate with the storage system and perform administrative functions. Network connectivity should already exist in environments where data sets over CIFS are in use.

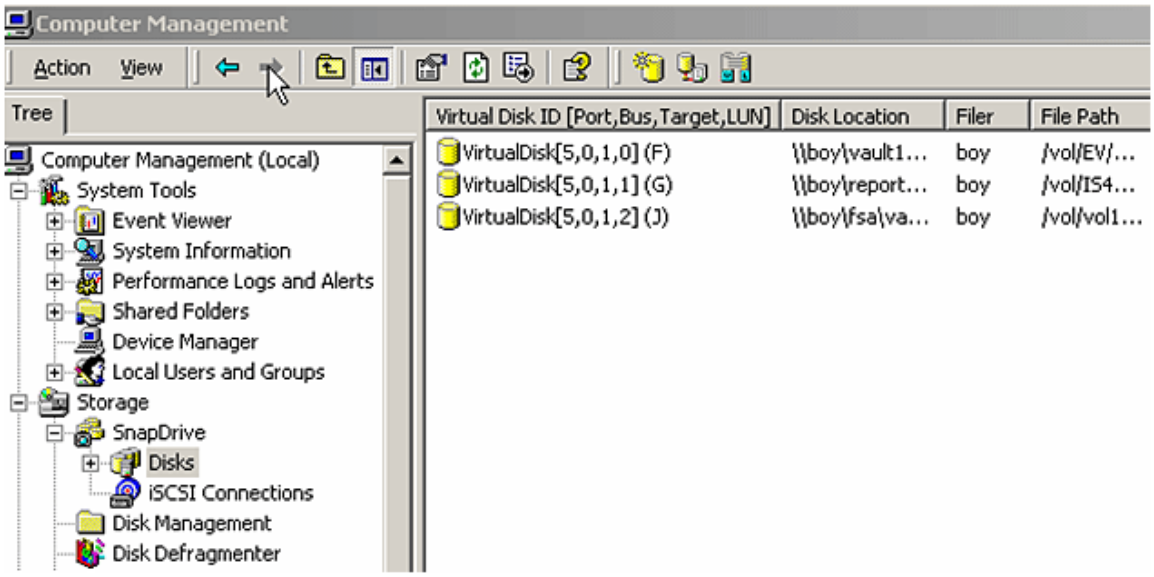

Figure 2) Storage configuration using SnapDrive tool.

In order to minimize the time and efforts to bring up the FileNet IS system at the remote location, it is important to maintain a similar setup at the remote site. This includes keeping the installation and data path similar to the primary system. Since a Windows server requires the registry information, it is useful to install and configure both SQL Server and FileNet IS server at the remote location. After the initial configuration and setup, both the SQL Server and FileNet IS services may be stopped to maintain data consistency. The following output shows a similar storage path used on the remote location server as the primary site server.

```
F:\>dir
 Volume in drive F has no label.
 Volume Serial Number is 5451-B2B6

 Directory of F:\

07/18/2005  03:08p      <DIR>          mssql8
06/09/2005  11:28a      <DIR>          temp
               0 File(s)              0 bytes
               2 Dir(s)   5,765,619,712 bytes free
```

```
F:\>dir g:
 Volume in drive G has no label.
 Volume Serial Number is 067D-D188

 Directory of G:\

07/18/2005  03:36p      <DIR>          FNSW
07/27/2005  11:39a      <DIR>          FNSW_LOC
07/11/2005  11:52a      <DIR>          temp
               0 File(s)              0 bytes
               3 Dir(s)  14,860,570,624 bytes free

F:\>dir j:
 Volume in drive J has no label.
 Volume Serial Number is C482-AF70

 Directory of J:\

07/18/2005  03:48p      <DIR>          data
05/20/2005  03:50p      <DIR>          ExchangeSP3
07/18/2005  03:48p      <DIR>          msar
               0 File(s)              0 bytes
               3 Dir(s)   2,460,913,664 bytes free

F:\>
```

Figure 3) Software configuration path on Windows server at destination site.

Note that the relevant LUNs are used in the local system to improve the ability to bring up the system quickly after a failure at the primary location. In Figure 4, three LUNs are used on the primary server.

LUN	Description	Size	Status	Maps Group : LUN ID
/vol/EV/EV/ev instal.lun		6.006 GB	online	viaRPC.iqn.1991-05.com.netapp:butthead : 0
/vol/EV/EV/vault.lun		4.006 GB	online	*No Maps*
/vol/IS40/report/report.lun		14.011 GB	online	viaRPC.iqn.1991-05.com.netapp:butthead : 1
/vol/vol1/SQL/sqldb.lun		2.007 GB	online	*No Maps*
/vol/vol1/fsa/pers		10.004 GB	online	*No Maps*
/vol/vol1/fsa1/ev instal.lun		6.006 GB	offline	*No Maps*
/vol/vol1/fsa1/vault.lun		4.006 GB	online	viaRPC.iqn.1991-05.com.netapp:butthead : 2
/vol/vol1/sql	SQL Server	2.007 GB	online	*No Maps*

Figure 4) NetApp storage volume details associated with LUN mapping information.

3.2. FileNet is on Windows Server

It is assumed that IS is installed and running at the primary location. FileNet supports Windows for installation and configuration of FileNet IS services. FileNet supports both UNIX and Windows platforms. Supported UNIX platforms are Solaris, HP/UX, and AIX. In our test configuration, we used a Windows platform. Similar NetApp storage configurations will also work for IS on HP/UX, AIX, and Solaris platforms, though specific settings will be different for other versions of UNIX. The patch requirements for UNIX platforms should be checked with FileNet documentation. Any discussion of UNIX platforms is beyond the scope of this document. FileNet supports Oracle and SQL Server. Our test environment used Windows, MSSQL 2000 with SP3, and Data ONTAP 7.0.1R1 with FileNet IS 4.0 software.

3.3. Verify at Primary Site

Once the installation process at the primary site is complete, verify that SQL Server and IS servers are up and running. It is important that the IS server is running with no error conditions.

In order to complete this task, check the SQL Server status using Enterprise Manager and then check the IS server status by seeing the event log. In our test setup, SQL Server status was checked, and it is shown in Figure 5.

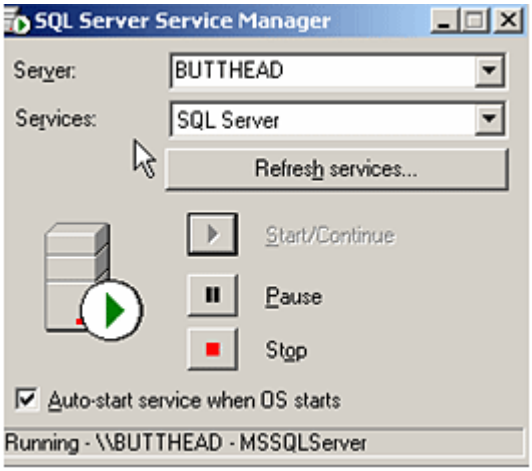

Figure 5) SQL Server status at primary site.

For quick and easy server recovery at the primary, it is important to add all the necessary network addresses of both FileNet IS server addresses. The entry on both servers should include the network addresses of the two servers. By configuring all the relevant addresses, FileNet IS will be able to verify the network address and come up quickly.

On our test setup, we included the network addresses used by the remote location server. Note that the network addresses listed here include the addresses of both servers.

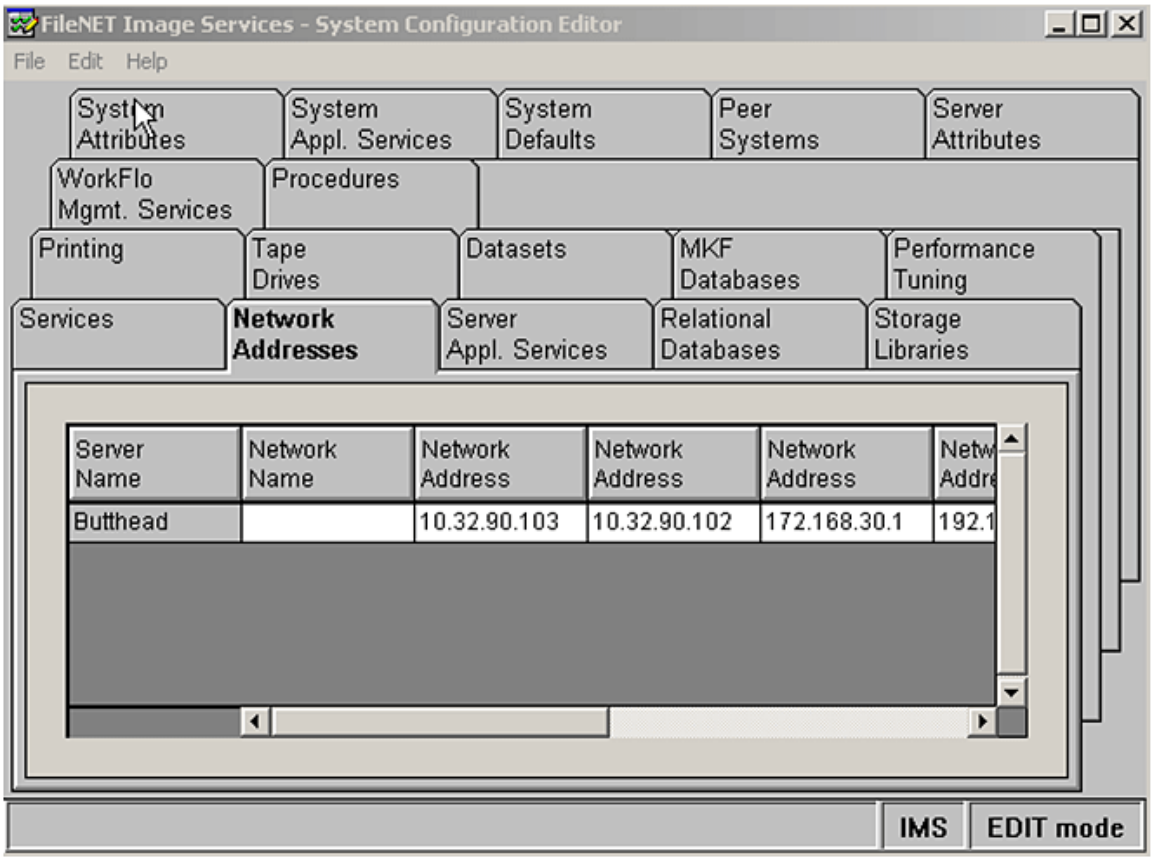

Figure 6) Network addresses displayed with configuration editor.

Once the network addresses are included in the configuration editor, verify that the data set path information matches with the other system. Figure 7 shows the path for configuring the FileNet IS data set path. This type of configuration is needed in a disaster recovery setup design plan.

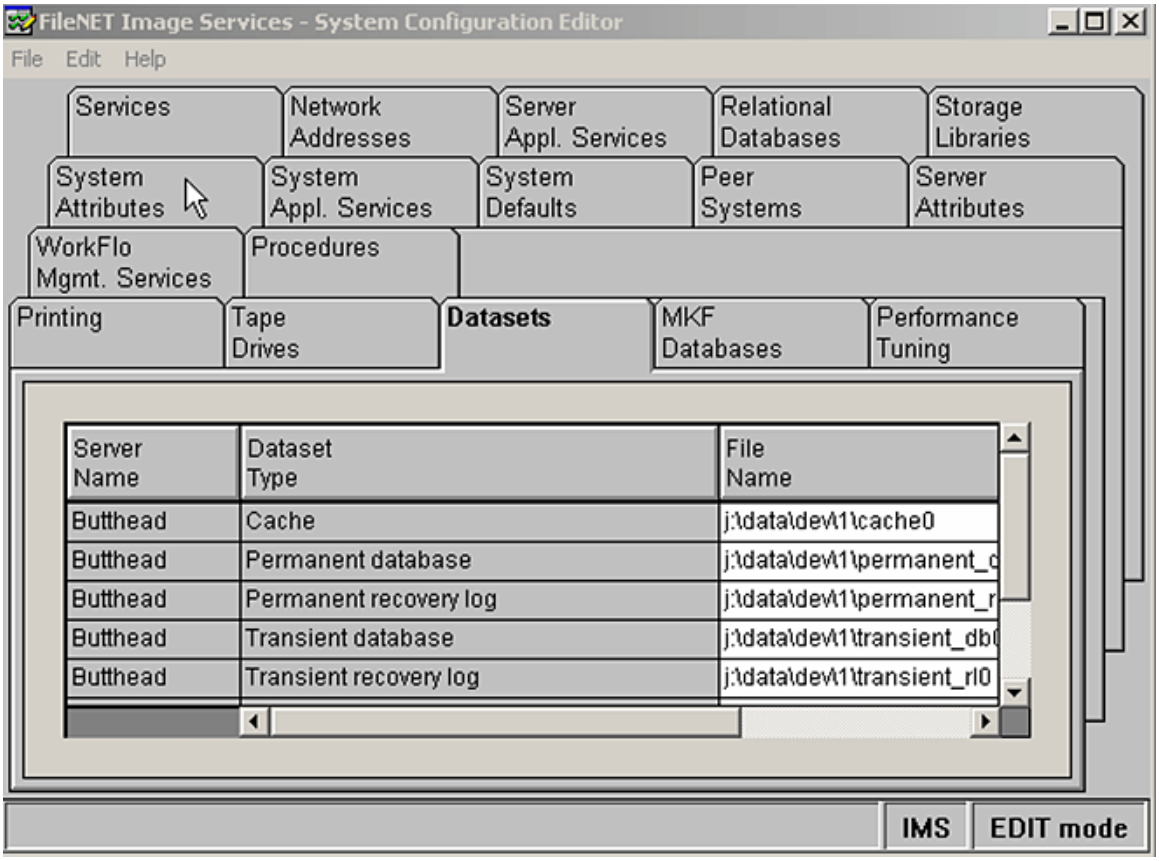

Figure 7) Data set path shown with configuration editor.

Once the setup is complete, our test setup verified that the FileNet IS services could be started successfully. To complete the checkup, we checked the hostname at the primary site and the ability to start the IS services. Output of these tasks is listed below:

```
F:\>hostname
Butthead

F:\>initfnsw status

Software status for host 'Butthead' (operating system = NT):
        Software stopped since 9/8/2005 3:23:27 PM

F:\>initfnsw start
Terminating processes...
Initializing FileNET software...
Starting index database...
```

```
Starting permanent database...
Starting transient database...
Starting security database...
Starting Courier...
Starting NCH_daemon...
Starting the Security Daemon...
Starting INXbg...
Starting INXu...
Starting document services...
Starting batch entry services...
Starting print services...
Startup of FileNET software initiated.  See event log for detailed status.

F:\>
```

After starting the services, check the event log to make sure the IS services are running without any issues. After that, attempt to log in to FileNet IS server using the Xapex utility as shown in Figure 8.

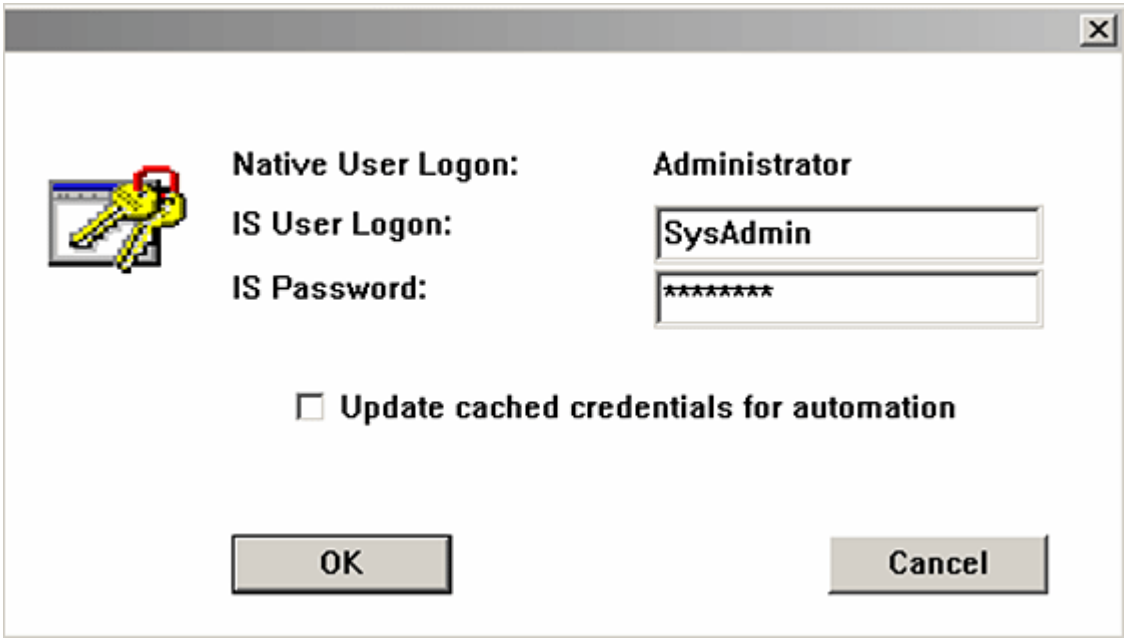

Figure 8) FileNet IS logon.

3.4 FileNet Image Service and the MSSQL Database Environmentat Destination Site

Both the MSSQL database and FileNet IS software are required to be installed at the destination site in a configuration similar to that of the primary site. This includes the drive letters being the same ones used in the primary site. This reduces complexity in bringing up the SQL Server and IS server at the destination site after the replication. As an example, our test setup used the following installation paths on the primary and destination sites:

```
F:>MSSQL for installing SQL Server software

F:>MSSQL\data for SQL Server Database data

G:>FNSW to install FileNet IS software

J:>dataset for FileNet IS data sets, including MKF, Primary, and TranLog
   data sets
```

Both systems used same version of SnapDrive software installed to manage the storage. This allows users to easily manage the storage component of the configuration.

Once these requirements are met, verify that SQL Server and FileNet IS servers can be brought up online and the data is in a consistent state. At this time, stop the FileNet IS and SQL Server at the destination site. Installation and configuration of SQL Server and FileNet IS server are required on the Windows server to have necessary registry information, which will help to bring up these services after the data replication from the primary site.

Figure 9 shows that a similar disk configuration was used on the server at the disaster recovery (DR) location. Note that the target storage system LUNs are configured to have similar drive letters to those on the primary server. This strategy will help to improve the ability to quickly bring up the server at the DR site.

Virtual Disk ID [Port,Bus,Target,LUN] (...	Disk Location	Filer	File Path
VirtualDisk[3,0,2,0] (F)	\\sunday\ev1\ev instal.lun	sun...	/vol/EV/EV/ev instal....
VirtualDisk[3,0,2,1] (G)	\\sunday\report\report....	sun...	/vol/pers/report/rep...
VirtualDisk[3,0,2,2] (J)	\\sunday\fsa1\vault.lun	sun...	/vol/sri1/fsa1/vault.lun

Figure 9) Storage configuration at disaster recovery site.

Once the storage configuration verification is complete, check the status of SQL Server. On our test setup, we used SQL Server Service Manager to check the status.

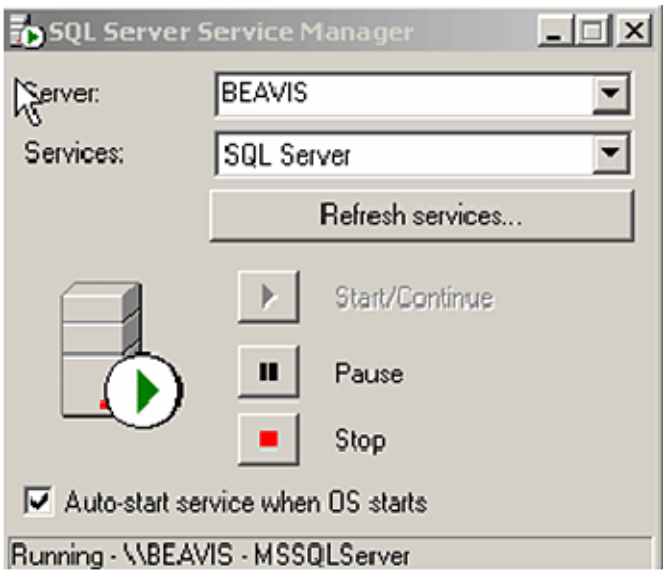

Figure 10) SQL Server Service Manager at DR site.

As explained previously in this section, make sure the storage path is available and configured similarly to the primary server.

```
Directory of j:\msar

07/18/2005  03:48p      <DIR>          .
07/18/2005  03:48p      <DIR>          ..
07/21/2005  04:49p      <DIR>          1
               0 File(s)              0 bytes
               3 Dir(s)   2,460,913,664 bytes free

G:\>dir
 Volume in drive G has no label.
 Volume Serial Number is 067D-D188

 Directory of G:\

07/18/2005  03:36p      <DIR>          FNSW
07/21/2005  04:49p      <DIR>          FNSW_LOC
07/11/2005  11:52a      <DIR>          temp
```

```
               0 File(s)              0 bytes
               3 Dir(s)  14,861,144,064 bytes free

G:\>dir f:\mssql8
 Volume in drive F has no label.
 Volume Serial Number is 5451-B2B6

 Directory of f:\mssql8

07/18/2005  03:08p      <DIR>          .
07/18/2005  03:08p      <DIR>          ..
07/18/2005  03:22p      <DIR>          MSSQL
               0 File(s)              0 bytes
               3 Dir(s)   5,765,619,712 bytes free
```

4. Data Replication

This section describes the procedure for configuring and data replication using a SnapMirror solution. For additional information on SnapMirror, refer to the product documentation available online. In order to replicate the data using SnapMirror, the storage devices have to be configured prior to the start of the replication process. The setup will allow configuring the source and the destination for replicating data between storage devices. Note that SnapMirror replicates data between NetApp storage devices. This means the source and the destination storage devices must be NetApp storage devices. The storage capacity on the destination location must be the same as or larger than the source device volume.

On our test setup, it was verified that the FileNet IS service can be started successfully without any errors, and it is shown in Figure 11.

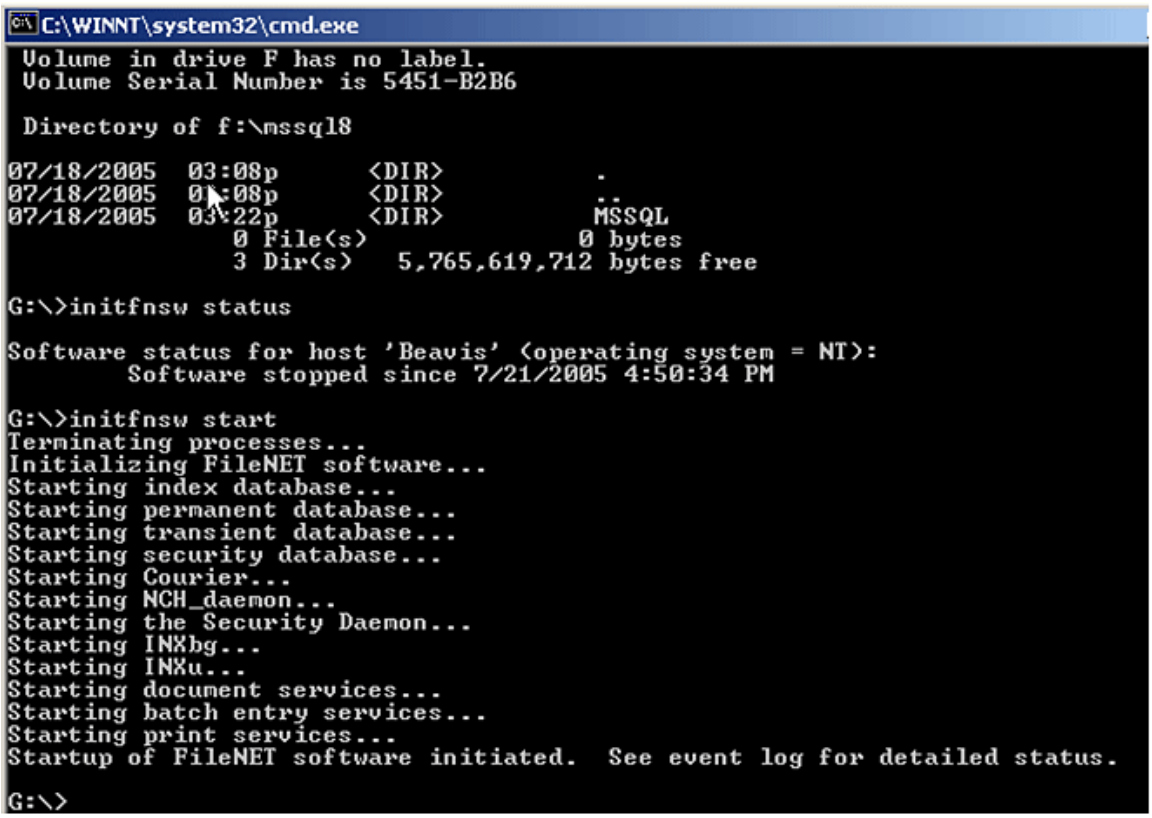

Figure 11) FileNet IS startup at DR site.

4.1 SnapMirror Configuration

SnapMirror configuration is required to set up the data replication process using SnapMirror. SnapMirror configuration provides all the information about the source and target location for data replication. Two files on the NetApp device have to be configured, and they are:

`/etc/snapmirror.allow`, which allows other NetApp devices to pull the data out of the source device during the SnapMirror process. It is recommended that all the NetApp devices that are involved in the replication process be included. This file may be edited either on a command prompt for a network share-mapped disk of the NetApp device root volume such as /vol/vol0 or on a storage system console. On our test setup, `/etc/snapmirror.allow` had the following content.

On NetApp storage system, the SnapMirror configuration on our system is as shown below.

```
boy> rdfile /etc/snapmirror.allow
#Regenerated by registry Fri Jul 8 01:21:12 GMT 2005
sunday
boy
```

Similarly, configure the source and destination path for data replication and enter the path information in /etc/snapmirror.config on both devices. On our test setup, we used the following configuration:

```
sunday> rdfile /etc/snapmirror.conf
#Regenerated by registry Thu Jul 21 23:16:43 GMT 2005
boy:/vol/EV/EV sunday:/vol/EV/EV restart=never 0 2 21 *
boy:/vol/IS40/report sunday:/vol/pers/report restart=never 0 2 21 *
boy:/vol/vol1/fsa1 sunday:/vol/sri1/fsa1 restart=never 0 2 21 *
sunday>
```

4.2 IS in Offline Mode

In order to minimize the time and efforts required to bring up IS at the destination site, replicating the data in offline mode is recommended. With that in mind, it is suggested that SQL Server be shut down and IS services be stopped. Once these services are offline, flush the system metadata by running tools such as sync.exe or similar programs. This flushes the metadata on the local disks and addresses the data consistency issue.

```
F:\>initfnsw stop
Are you sure you want to stop software on server 'Butthead'? (y|n)[n]: y
Terminating FileNET software...
Shutting down transient database...
Shutting down permanent database...
Shutting down security database...
Terminating processes...
Shutting down index database...
Termination of FileNET software completed.

G:\>initfnsw status

Software status for host 'Butthead' (operating system = NT):
        Software started since 9/8/2005 3:34:35 PM

G:\>
```

Show the output of flushing the metadata. Run a script or your program to flush the system metadata. On our test setup, flushing of the metadata is shown below for all available local disks on the Windows server.

```
Flushing: C E F G J
C:\Temp>
```

4.3 Prepare for Data Replication

Once the SQL Server and FileNet IS services are stopped at the destination site, using the SnapDrive tool, disconnect the LUN used to connect the SQL Server, IS Server, and data sets. Verify that the LUNs on the destination server are disconnected and the LUNs are unmapped. By following procedure, data from the source may be replicated to the target location. At this time, put the destination volume in restricted mode and create a Snapshot copy of the source volume. Creating the Snapshot copy quickly allows you to bring the system online. In our test setup, we allowed the data to be replicated completed as a base copy for the first time and then allowed incremental data change replication.

It is important to stop the SQL Server and IS at the DR site and certain storage management tasks to be completed before starting the replication using SnapMirror. This includes flushing the system metadata and disconnecting the local disks that were connected using SnapDrive tool. By disconnecting the disk drives, data can be replicated from the source.

Defining the replication path by providing the source and destination storage system path would help to replicate the data from the source to the destination NetApp storage system. On our setup, "boy" was the source device, and the data was replicated from boy to another NetApp storage device called "Sunday." The following output shows the current destination path for replication.

```
Current Destinations: on "boy" storage system
Path       Destination
/vol/EV/EV sunday:/vol/EV/EV
/vol/IS40/report sunday:/vol/pers/report
/vol/vol1/fsa1 sunday:/vol/sri1/fsa1
```

Initialize the replication process by issuing the "snapmirror initialize" command and provide the path for data at the source location to the destination site.

4. 4 Break the SnapMirror Replication

Once the data is replicated as a base copy, the replication process may be stopped or continue to have data replicated to the destination path. If the data is continued to be replicated after the initial copy, the destination recovery process requires additional tasks to bring up the IS to a consistent state. This may be done using the dbverify utility tool provided by FileNet IS software. In our test setup, we used a base-level data replication that will not require any additional recovery efforts to bring up the services at a disaster site.

Once the base-level data replication is complete, break the SnapMirror replication. The status of SnapMirror may be verified by using "snapmirrror status" on the NetApp storage device.

4.5 Reconnect the LUNS Using SnapDrive

New LUNs replicated from the source NetApp devices are ready to be configured and connected to the destination server. In order to successfully reconnect the LUNs, existing LUN mapping information has to be removed. Using the SnapDrive tool, reconnect the LUNs with the same drive letter as the source NetApp device. An example would be F:\ for the LUN that replicated the SQL Server data.

Before reconnecting the LUNs at the destination site, certain tasks must be completed. The LUNs replicated from the primary system will reflect the mapping information of the source system. Unmap these settings and bring it online. Once it is ready to be configured as the local disk, the SnapDrive tool may be used to reconnect the local disks. On our setup, we verified that no relevant NetApp storage devices were connected, and it was verified as shown in Figure 12.

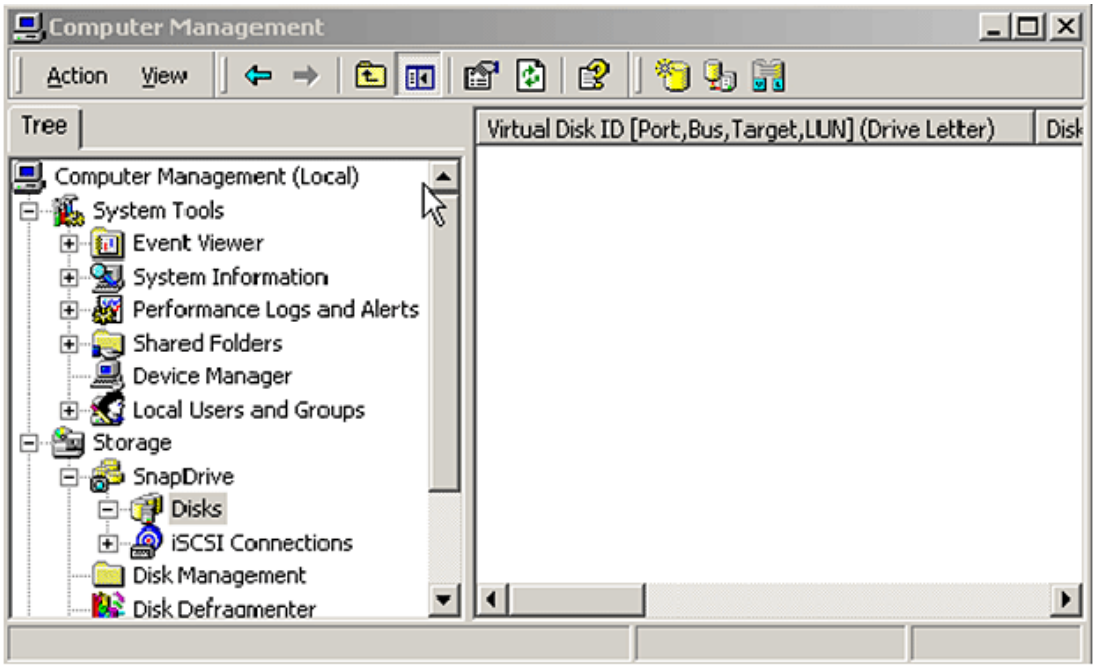

Figure 12) Computer management before local disk configuration.

Using the SnapDrive tool, reconnect the local disks by selecting the appropriate LUNs and the UNC path as shown in Figure 13.

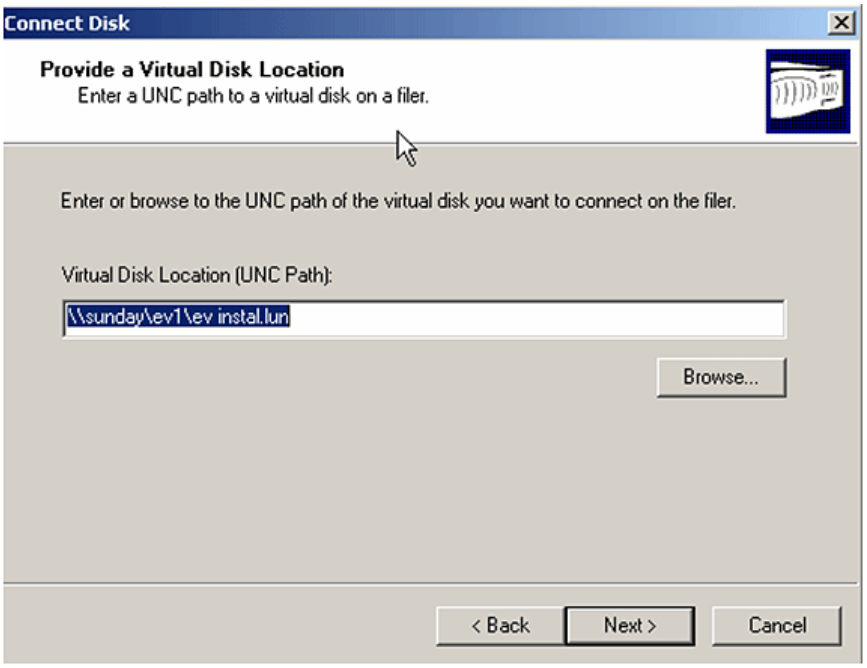

Figure 13) Reconnecting virtual disk.

During the reconnection task, verify the UNC path, disk size, disk protocol type, and (very important) the drive letter, as shown in Figure 14.

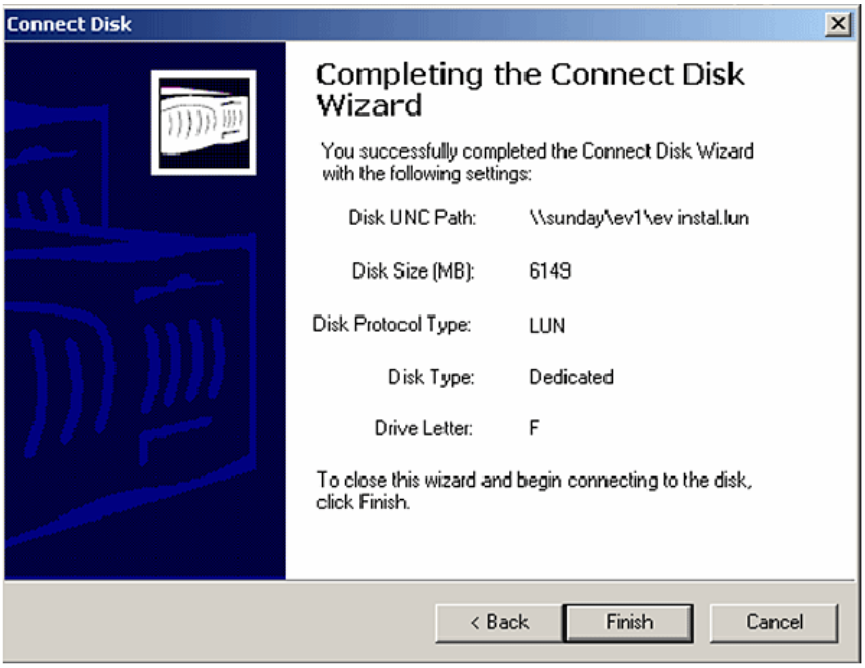

Figure 14) Reconnecting local disk after replication.

Repeat reconnecting the disks for all the remaining replicated paths (LUNs). On our system reconnected disks successfully were as shown in Figure 15.

Virtual Disk ID [Port,Bus,Target,LUN] (Drive Letter)	Disk Location	Filer	File Path	Backed By File Path	Disk
VirtualDisk[3,0,2,0] (F)	\\sunday\ev…	sun…	/vol/EV/…		LUN
VirtualDisk[3,0,2,1] (G)	\\sunday\rep…	sun…	/vol/per…		LUN
VirtualDisk[3,0,2,2] (J)	\\sunday\fsa…	sun…	/vol/sri1…		LUN

Figure 15) Reconnected disk path information

5. Starting Servers at Destination Site

Once the LUNs are mapped and reconnected with the drive letter, verify that the related files are visible. This can be simply verified with the "dir" command. The first step would be to start the SQL Server and then start the IS Control Service using the administration tools. Then verify that the IP address of the new Windows server is included in the FileNet IS server using the fn_edit tool.

Before starting the FileNet IS services, verify that all the required storage paths are available. Now use the FileNet configuration editor to verify that the network addresses and the data set paths are similar to the original configuration. In our setup, the FileNet configuration editor shows the server name as "Butthead" on the DR system. This is not an issue to start FileNet IS. Once the server is started, it will be recognized on the DR system as the "Beavis" server.

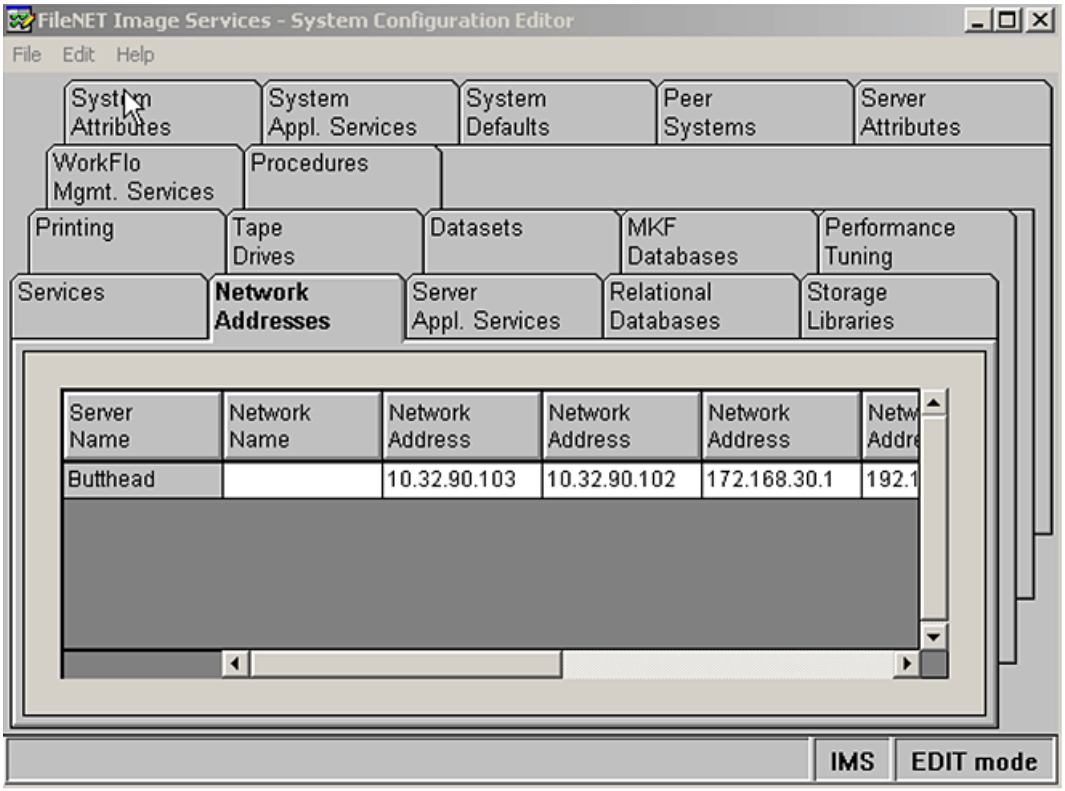

Figure 16) Network addresses on the replicated system.

Start the SQL Server and verify that it is started successfully. Before starting IS, verify that the path for data sets, including the path for MKF, is accessible. Now start the IS and monitor the status using the event log. Observe carefully to verify that the IS is started without any errors. If a database verification error is noticed while starting FileNet IS, it could be due to document inconsistency in the IS server. This error may be addressed by checking what documents were committed into FileNet system and the documents that did not make it to the system. Use the FileNet IS tools to remove the document numbers that are entered and the data that was not committed. These documents may be reentered into the system manually from the cache or manually. Please contact the FileNet professional services team for further assistance.

```
J:\>initfnsw status


Software status for host "Beavis" (operating system = NT):
        Software stopped since 9/9/2005 3:07:12 PM


J:\>


J:\>initfnsw status


Software status for host "Beavis" (operating system = NT):
        Software stopped since 9/9/2005 3:07:12 PM


J:\>initfnsw start
Terminating processes...
Initializing FileNET software...
Starting index database...
Starting permanent database...
Starting transient database...
Starting security database...
Starting Courier...
Starting NCH_daemon...
Starting the Security Daemon...
Starting INXbg...
Starting INXu...
Starting document services...
Starting batch entry services...
Starting print services...
Startup of FileNET software initiated. See event log for detailed status.
```

```
J:\>
```

After starting the IS, check the events log for any errors. If the data was replicated in offline mode, IS services come up successfully without involving much effort. If the IS is started without any issues, log in to the IS system by using the Application Executive utility tool to make sure a user can log on to the FileNet IS server. On our setup, this was verified by logging into the system as shown in Figure 17.

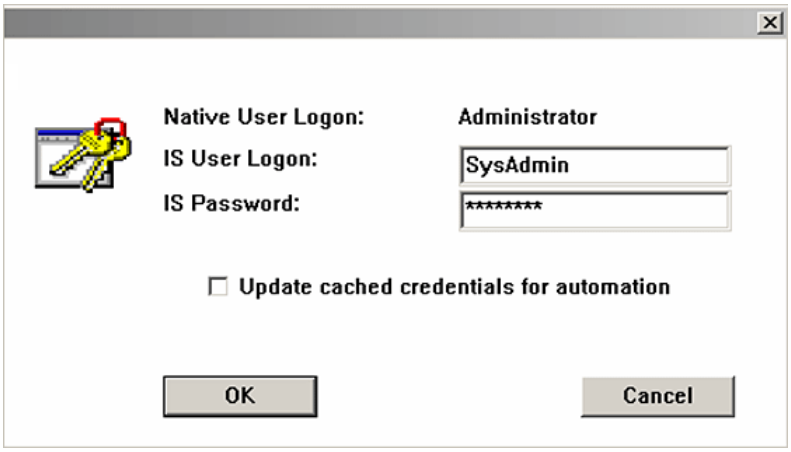

Figure 17) FileNet IS user logon.

After logging on, Application Executive provides a status as shown in Figure 18.

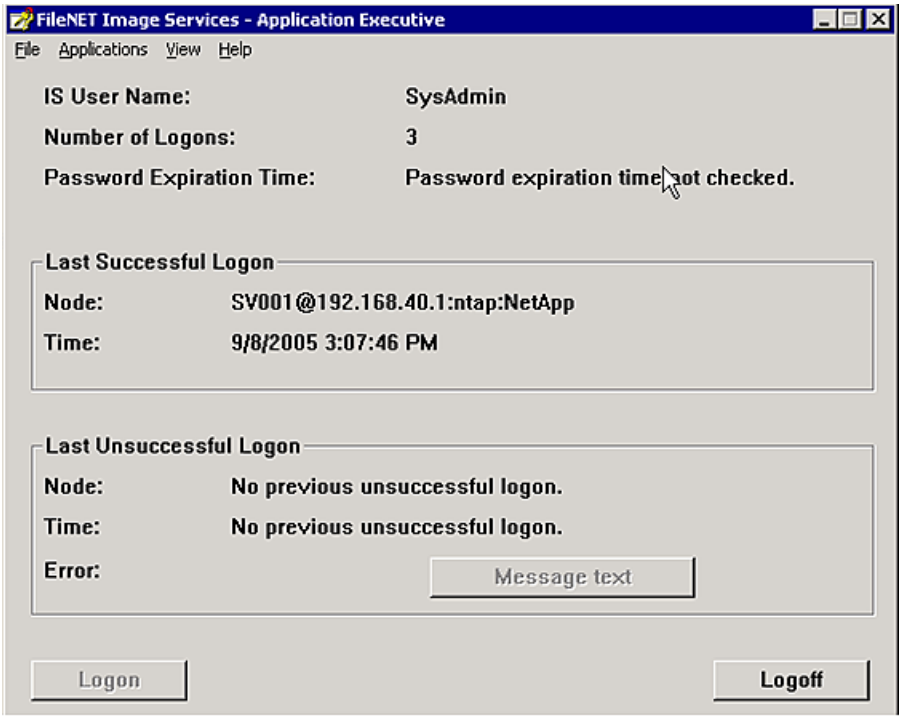

Figure 18) Application Executive logon status.

6. Integration of IS for SnapLock

To take advantage of WORM capability on magnetic media, FileNet has announced support for NetApp SnapLock via SSAR, which works with IS 4.0 servers. To take advantage of native retrieval, this paper recommends upgrading to IS 4.0 SP01 or later.

SnapLock configuration allows users to archive the data onto permanent nonerasable, nonrewritable magnetic media while taking advantage of NetApp technology for archival, backup, and disaster recovery. For detailed instructions on integrating IS Connector for SnapLock, refer to the upcoming technical report. Using SnapLock configuration, you will be able configure SSAR for compliance purposes.

Procedure to configure SSAR is described in "Integrating FileNet Image Services Connector for SnapLock with NetApp Storage."

7. Conclusions

FileNet support for image storage on magnetic disk using MSAR combined with NetApp unified storage enables NetApp storage systems to operate in a true unified storage architecture and serve as both file system and raw partition storage for FileNet IS, depending on the needs of the system and the preferences of the FileNet administrator. Administrators who need the features of SAN or NAS configurations (block or raw partition storage from SAN and remote file system storage from NAS on UNIX platforms) can now deploy FileNet storage that is fast, scalable, reliable, and flexible enough to store any kind of FileNet data, including database, MKF, cache, and images with MSAR. On Windows 2000, MKF/cache can be configured on network share devices. In addition, NetApp storage system integration provides FileNet customers with quick backup and recovery capabilities as well as simplified data replication and disaster recovery planning. This paper demonstrates that deploying NetApp unified storage solutions for FileNet storage is both technically simple and provides significant technical and business benefits when compared to traditional direct-attached, NAS-only, SAN-only, or optical storage.

The Network Appliance storage systems can provide large amounts of storage to FileNet applications. This storage can be managed in a way that will maximize I/O throughput.

Additionally, the use of FCP or iSCSI LUNs defined on a NetApp storage system volume can be used to provide large amounts of data space as well as combine multiple LUNs to service different systems or users.

Finally, the use of the NetApp storage system as a file-sharing appliance can consolidate data from various SAS data repositories. NetApp storage management software can be leveraged to control multiple storage systems at a single control point, making the overall management of storage simpler.

8. Caveats

NetApp has not tested all possible combinations of hardware platforms and storage architecture and software options. If you use a different server OS, different version of IS, or different database, significant differences in your configurations may alter the procedures necessary to achieve the objectives outlined in this document. Content and methods and procedures described are for informational purposes only. If you find that any of these procedures is inconsistent or if you need additional information, please contact the author immediately.

9. References

There are several technical papers related to SAN configuration available in the NetApp technical library. In addition to those papers, see the following documents:

Image Services Installation and Configuration Procedures for Windows, Release 4.0

MSAR Procedures and Guidelines for Image Services from FileNet Inc.

Data ONTAP 7.0.1 System Administrator's Guide

Microsoft SQL Server 2000: Implementing MSCS and SQL Server 2000 Virtual Server with a NetApp Filer

SnapManager for Microsoft SQL Server 2000 Best Practices

Network Appliance: Data ONTAP Administration Guide, available at now.netapp.com

Network Appliance: SnapDrive Installation Guide

Network Appliance technical report: iSCSI: Accelerating the Transition of Network Storage

Network Appliance technical report: Windows 2000 and NetApp Filers: An Overview