Disaster Tolerance and Data Availability

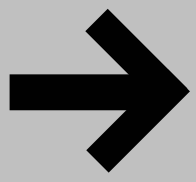
ESG472LG0303

lab

guide

Disaster Tolerance and Data Availability

ESG472LG0303



training

Disaster Tolerance and Data Availability
Lab Guide
March 2003

Lab 1 — HP OpenView Storage Virtual replicator

Lab 2 — HP StorageWorks Enterprise Volume Manager

Lab 3 — HP StorageWorks Secure Path for DRM

Lab 4 — HP StorageWorks Data Replication Manager Installation

Lab 5 — Scripting HP StorageWorks Data Replication Manager

Addendum 1 — HP StorageWorks Secure Path 3.1 for Windows lab

Objective

Your customer, Widget Inc., is interested in using HP OpenView Storage Virtual Replicator to allow the quick backup of their SQL database. Their current backup window is not at an acceptable time threshold. They want to use Virtual Replicator to create snapshots of their data to be used for online backups. Virtual Replicator will allow them to quickly backup their data, while not interrupting their applications.

The instructions in this lab take you through all the steps necessary to configure and use Virtual Replicator with Microsoft Windows 2000.

Note

You will find additional information in the Virtual Replicator System Administrator's Guide.

Hardware

Each group of students performing this lab requires one system configured as follows:

- Processor: Intel Pentium
- Memory: 128MB required (256MB recommended)
- Disk space: 100MB required for full Virtual Replicator installation
- Storage (one of the following configurations):
  - Internal — Four disk drives (one system disk, three unformatted drives). Three drives installed in the storage cabinet, one external to the cabinet.
  - External — Three disk drives (unformatted). JBOD LUNs created for two drives, one unassigned.

> **!** **Important**
> If you are using external HSG storage, ensure that you DILX the units to remove any existing OS metadata.

Preinstalled Software

The following software must be pre-installed:

- Microsoft Windows 2000, Professional, Server, or Advanced Server SP2 or greater for all versions.

> **Note**
> Virtual Replicator also supports Windows NT 4.0, SP6a or greater. However, the section on Online Volume Expansion requires Windows 2000.

- Microsoft Internet Explorer 5.01 or greater
- Microsoft Management Console 1.1 or greater
- Microsoft SQL Server 7 Service Pack 3 or greater.
- Parameters to use when setting up SQL Server 7:
  - Use a local service account
  - Select 50 Client Access Licenses
  - Using SQL Enterprise Administrator, ensure that authentication is set to both Windows NT and SQL. Select *Server* → *Properties* → *Security* → *Windows NT and SQL*.
- A SQL admin user created who has full rights to the *master* database. (The admin user can be created in SQL Enterprise Manager.)
- SQL "admin" user parameters include:
  - No password
  - All roles on the server
  - All access to the master database
- A c:\scripts directory on the local drive of each of server to install and run SQL scripts

> **Note**
> Microsoft Management Console (MMC) is included with the Windows 2000 operating system, but not with Windows NT 4.0. To obtain the latest version of MMC, contact Microsoft.

Virtual Replicator Lab Overview

Each section of the lab contains multiple exercises.

> **Note**
> The exercises in this lab use a GUI to execute Virtual Replicator tasks. To schedule a snapshot creation that will be used for backup, use the Virtual Replicator command line interface SnapMgr in a batch and use Windows Scheduler to schedule the execution of the batch.

Section 1 — Creating Pools and Virtual Disks

In this section, you will create pools and virtual disks using both the MMC and the command line interface.

Section 2 — Using Snapshots for Data Recovery

In this section, you will use snapshots to restore data from a corrupted database application. You will also simulate a drive failure and the resultant inability to recover if no external backup media is used.

Section 3 — Using Online Volume Growth (Optional)

In this section, you will learn about the new Online Volume Growth feature of Virtual Replicator for Windows 2000. You will expand a virtual disk dynamically while applications and data remain accessible.

Section 4 — Deleting Virtual Disks, Snapshots, and Pools

In this section, you will learn the proper procedure for removing snapshots, virtual disks, and pools.

Section 1 — Creating Pools, Virtual Disks

Overview

There are two exercises in this section:

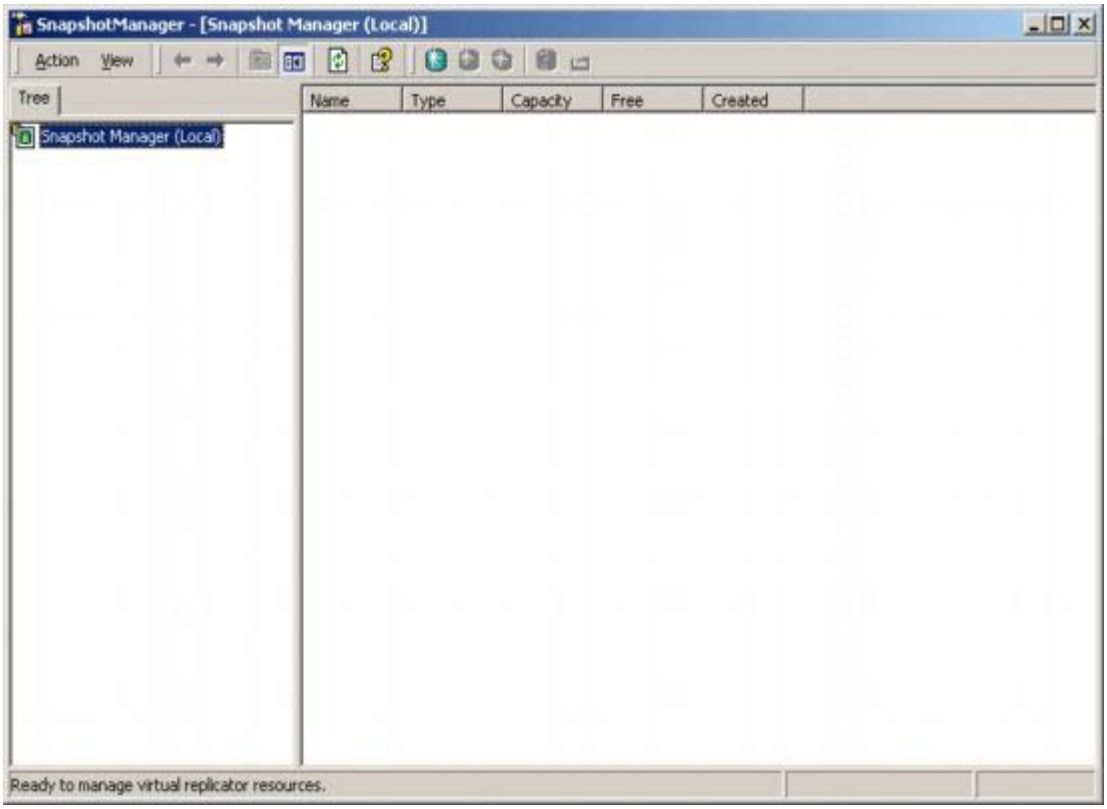
- Exercise 1: Creating Pools
- Exercise 2: Creating Virtual Disks

Exercise 1: Creating Pools

With Virtual Replicator, hardware array storage or physical disks are grouped into a logically concatenated pool of disk space. You can create any number of pools and use any storage to which Windows has direct access in a pool. In addition to standard single disks, you can use controller-based, fault-tolerant disk arrays, referred to as *storage units*.

The purpose of this exercise is to create a storage pool.

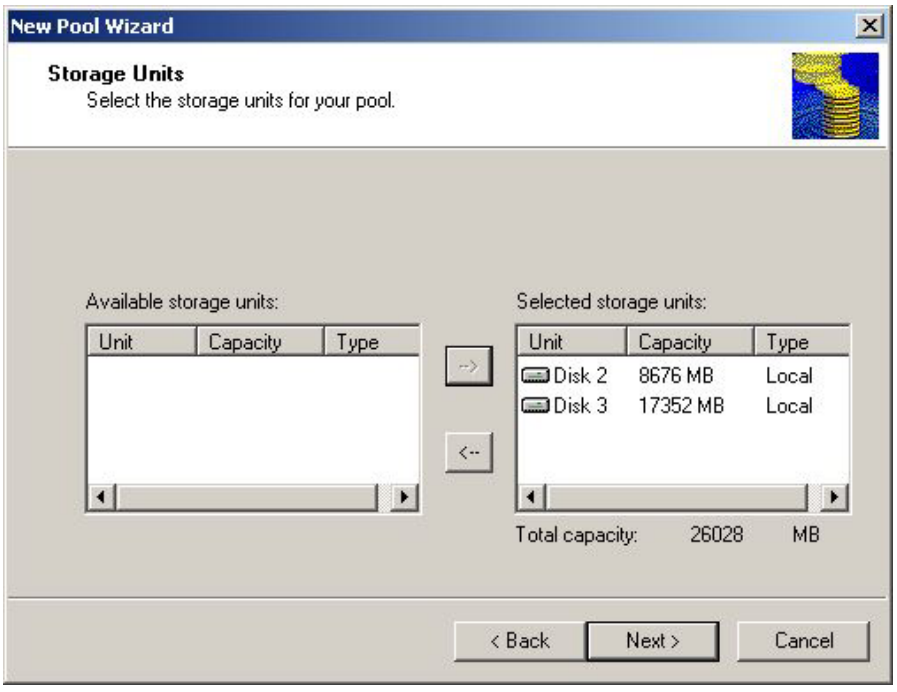
1. Start Virtual Replicator by selecting *Start* → *Programs* → *Compaq SANworks Virtual Replicator* → *Snapshot Manager*.



2. Right-click *Snapshot Manager (Local)* then select *New* → *Pool*.

3. Click *Next* when the New Pool Wizard displays.

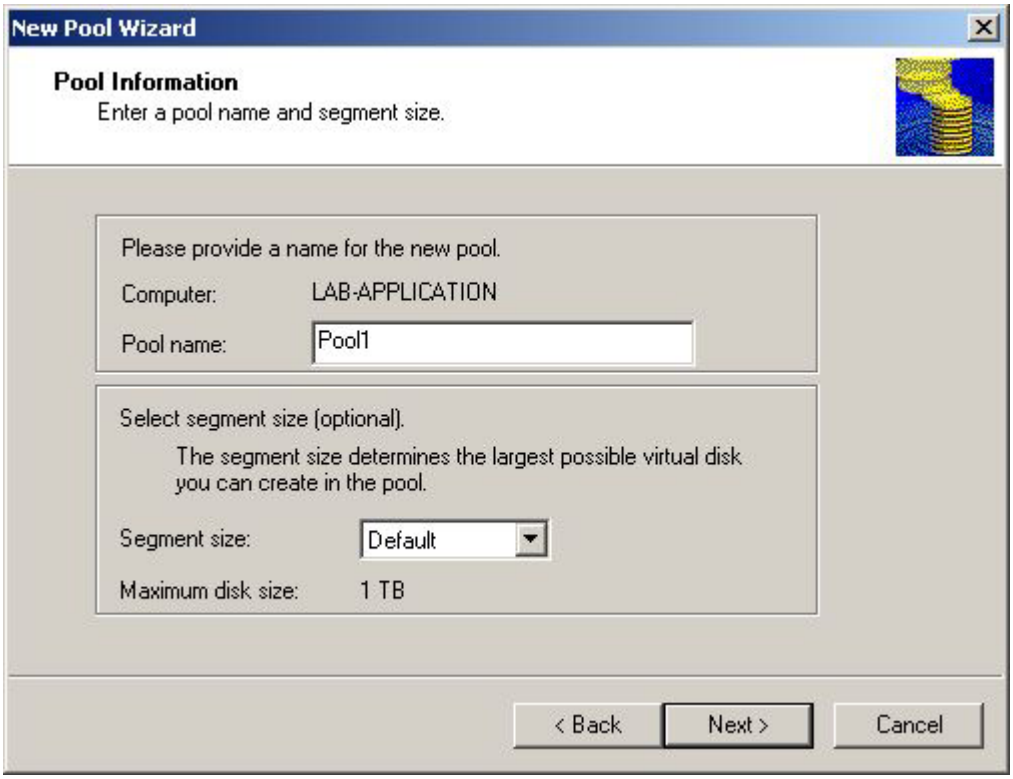
   The New Pool Wizard displays a list of storage units that are available for pool creation.



4. Select one of the storage units and click the right arrow button (→). Repeat this for the remaining storage units. Click *Next*. The Pool Information window displays.

   In the preceding screen shot, which storage units will be used in creating the pool?

   .....



5. Name the pool *Pool1*.

6. In the *Segment size* drop-down box, click each of the available options and note the corresponding *Maximum disk size.* A segment is a unit of disk space used in virtual disk allocation and snapshot copy-out operations.

   What are the available options for *Segment size*?

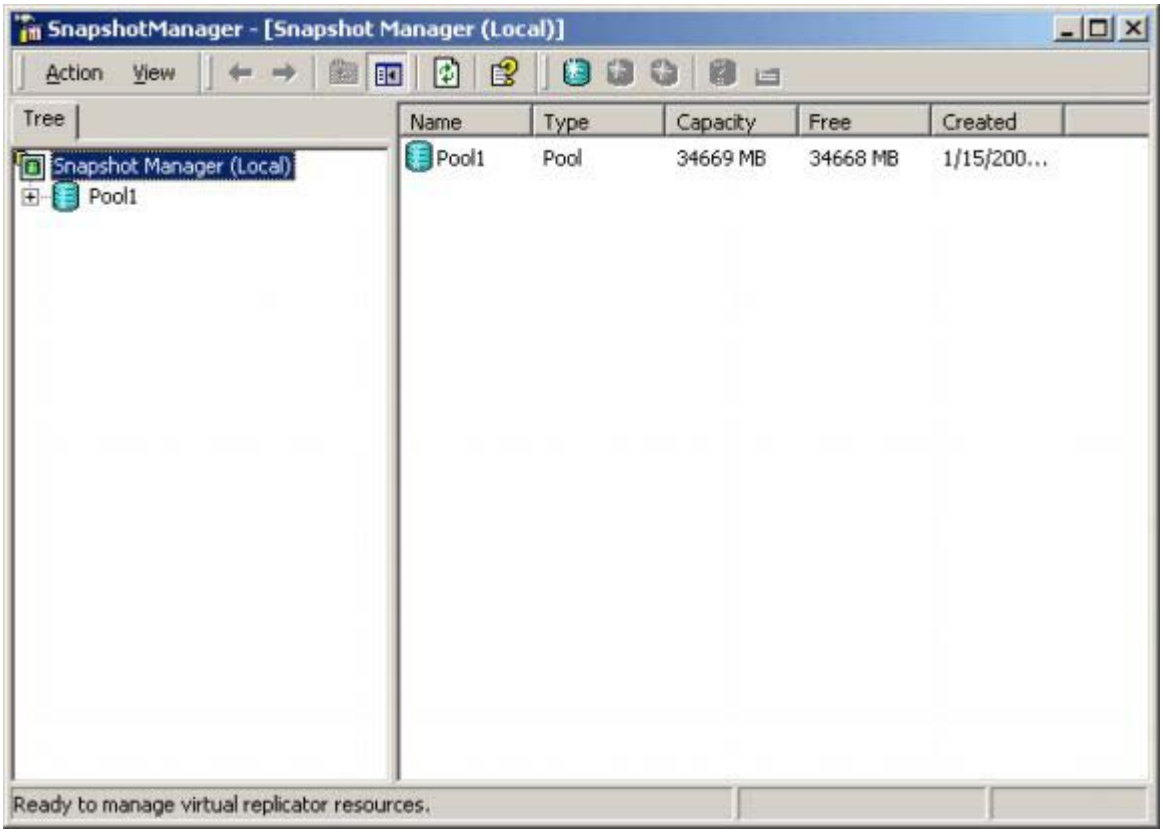
   .....

   What is the maximum disk size if 256KB is used for the segment size?

   .....

7. Select 128KB as the segment size, and click *Next*.

8. When the New Pool Wizard completes, click *Finish*.



On the MMC display, note that the newly created pool is listed in the window on the right side.

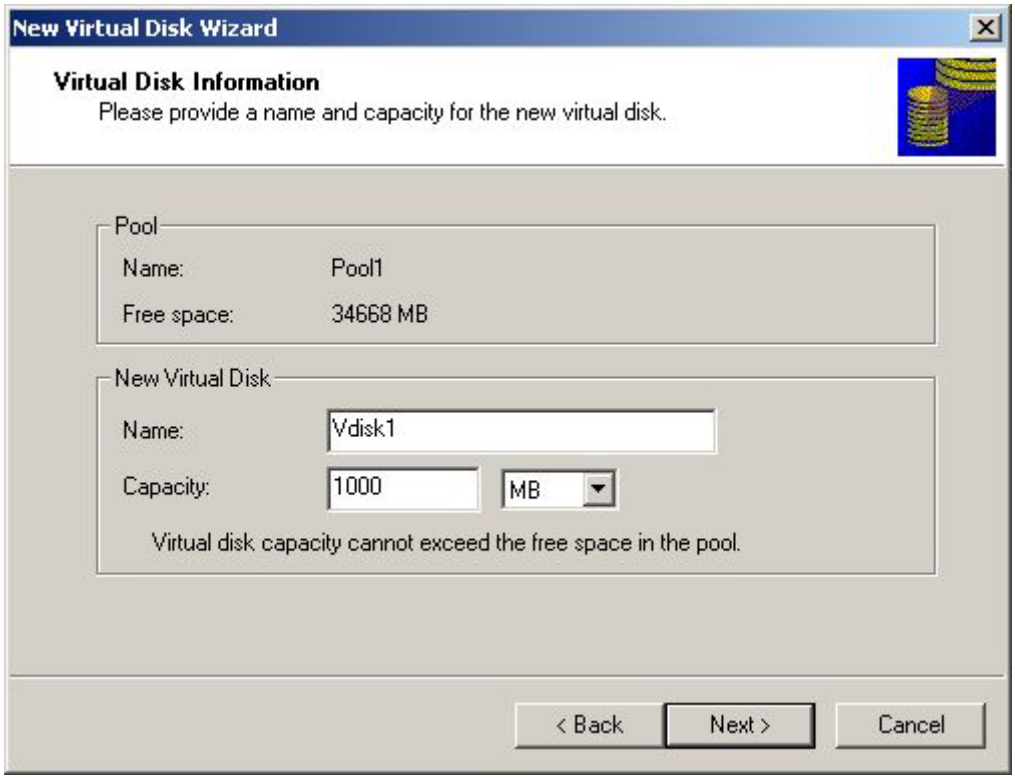
Exercise 2: Creating Virtual Disks

The virtual disks that you create in the pool perform and behave in exactly the same way as physical disks. That is, you can format and map drive letters to them, just like physical disks. You can also install applications to a virtual disk, including cluster-aware applications, such as Microsoft Exchange.

To create virtual disks.

1. Open Snapshot Manager.
2. Right-click *Pool1*.
3. Select *New* → *Virtual disk.*

4. When the New Virtual Disk Wizard displays, click *Next*.

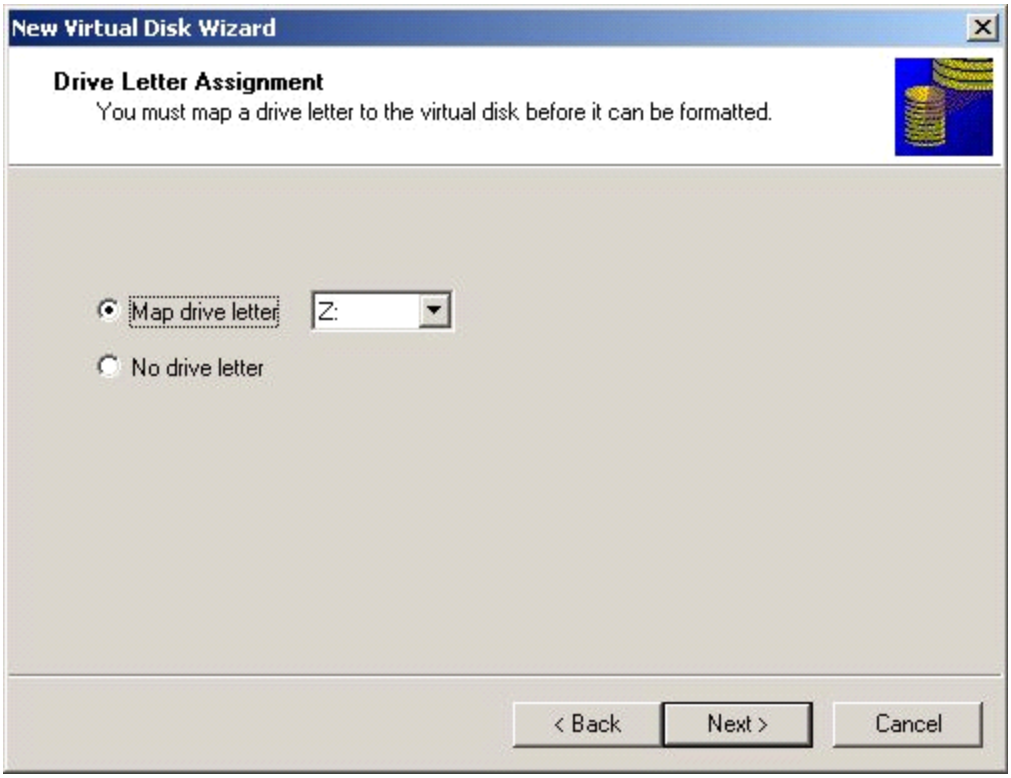


5. On the Virtual Disk Information screen, enter the new virtual disk name as *Vdisk1*.

   The name you select can be up to 23 characters long. Choose a name that is different from any pool or virtual disk on the stand-alone computer or cluster that you will be managing.

6. Enter a capacity value of *1000 MB* (1GB).

7. Click *Next*.

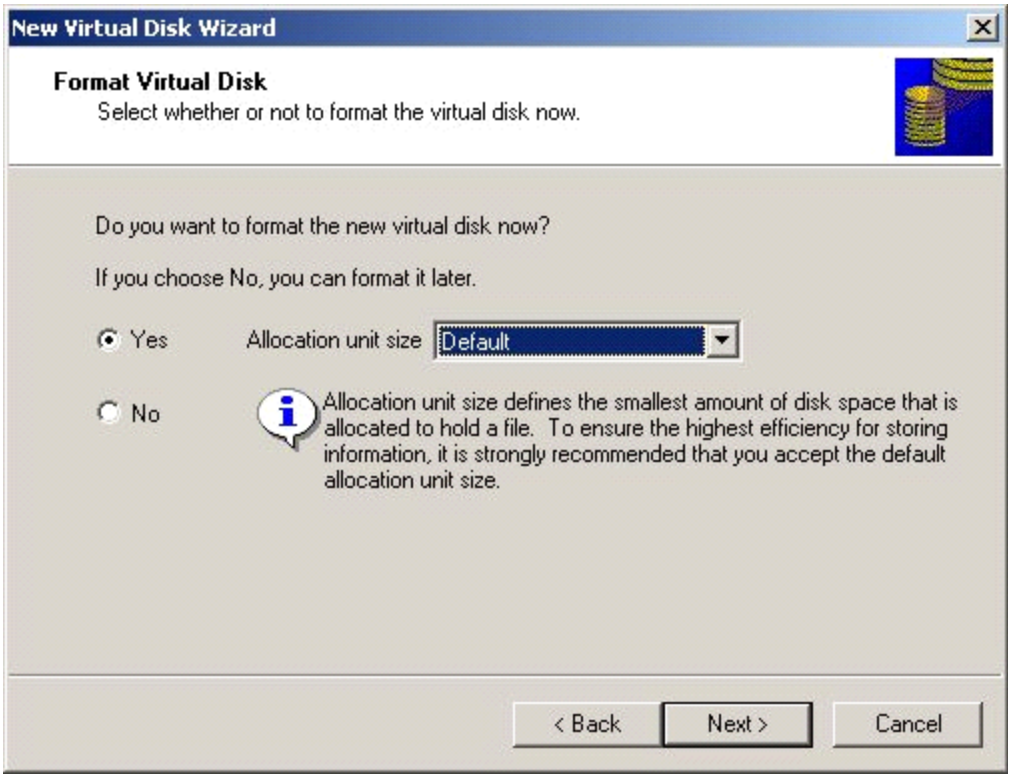


8. The Drive Letter Assignment window displays. Assign the drive letter *Z:* and click *Next*.

   What would be a reason for not assigning a drive letter at this time?

   .....

   .....



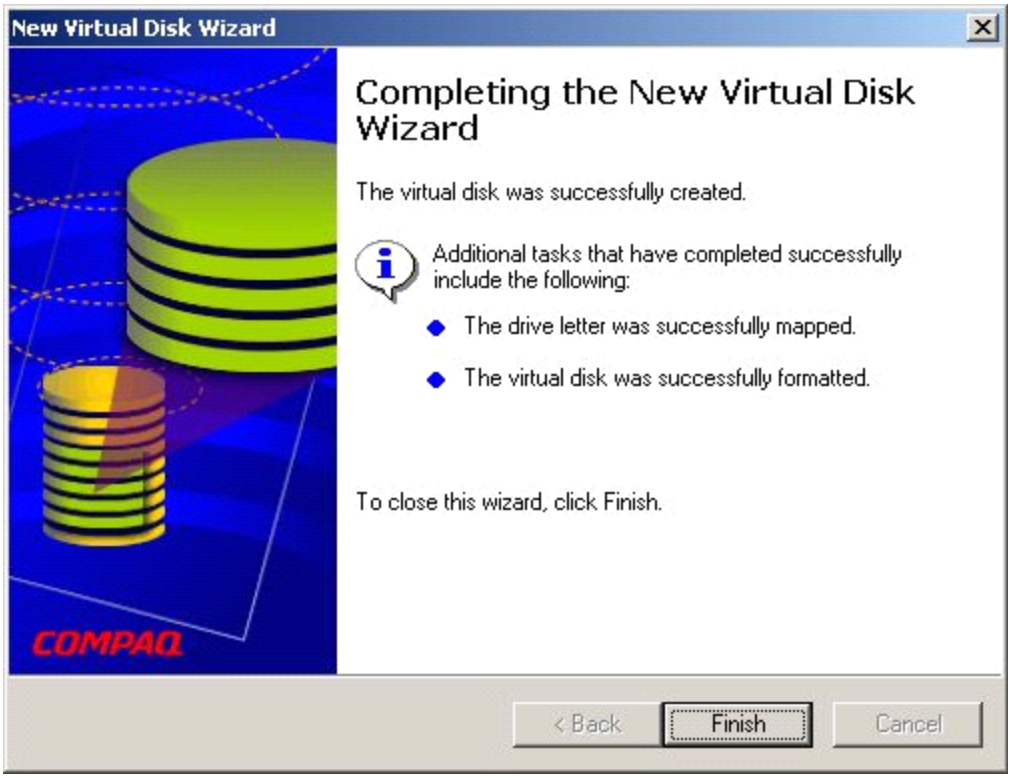
9. Ensure that *Yes* is selected on the Format Virtual Disk window.
10. Accept the default Allocation unit size (1024).

    Other than the reason listed on the screen, why should you select the default allocation size?

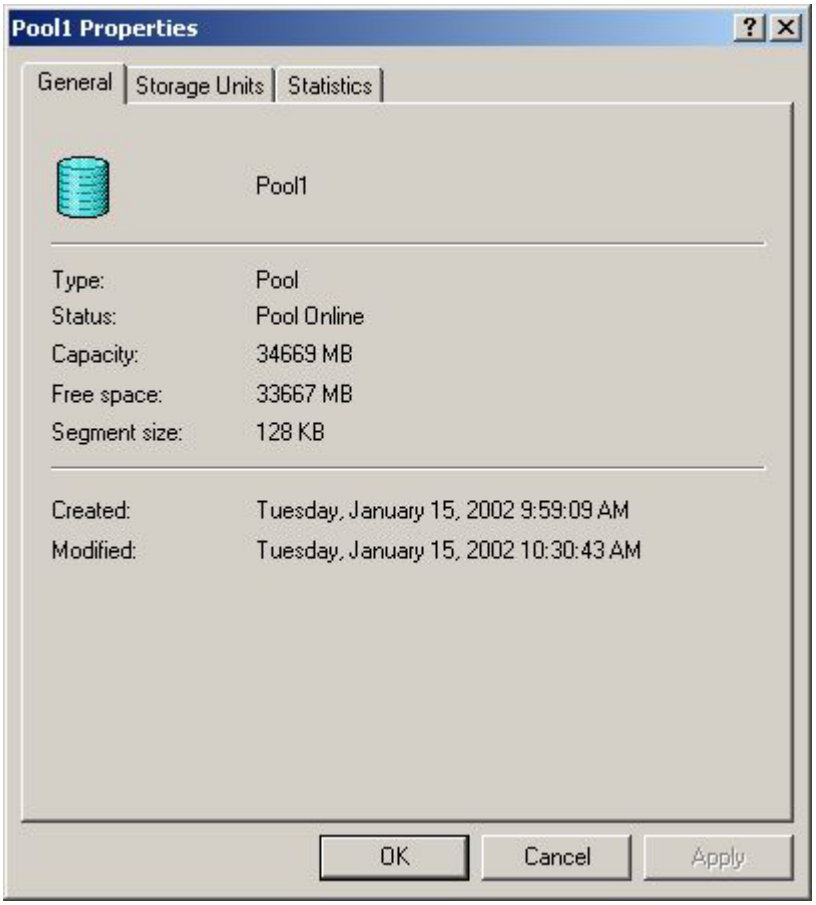
    .....

    .....

    (Hint: from the Virtual Replicator System Administrator's Guide, You cannot defragment a virtual disk if the allocation size is greater than 4096.)
11. Click *Next*.



12. Click *Finish.*
13. Click on *Pool1* and verify that the virtual disk that you created is listed under the pool and on the right side of the screen.



14. Right-click *Pool1* and select *Properties*.

    What storage units are included in the pool?

    .....

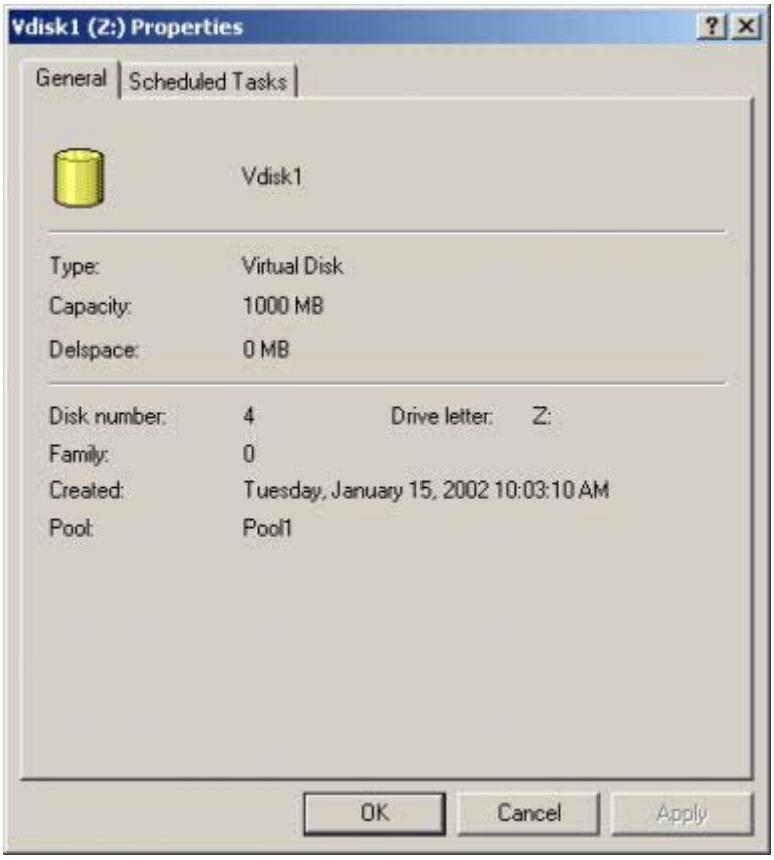
    What are the statistics for read and write operations?

    .....

    .....

    .....

15. Examine the information on each tab. Click *OK* when you are finished.

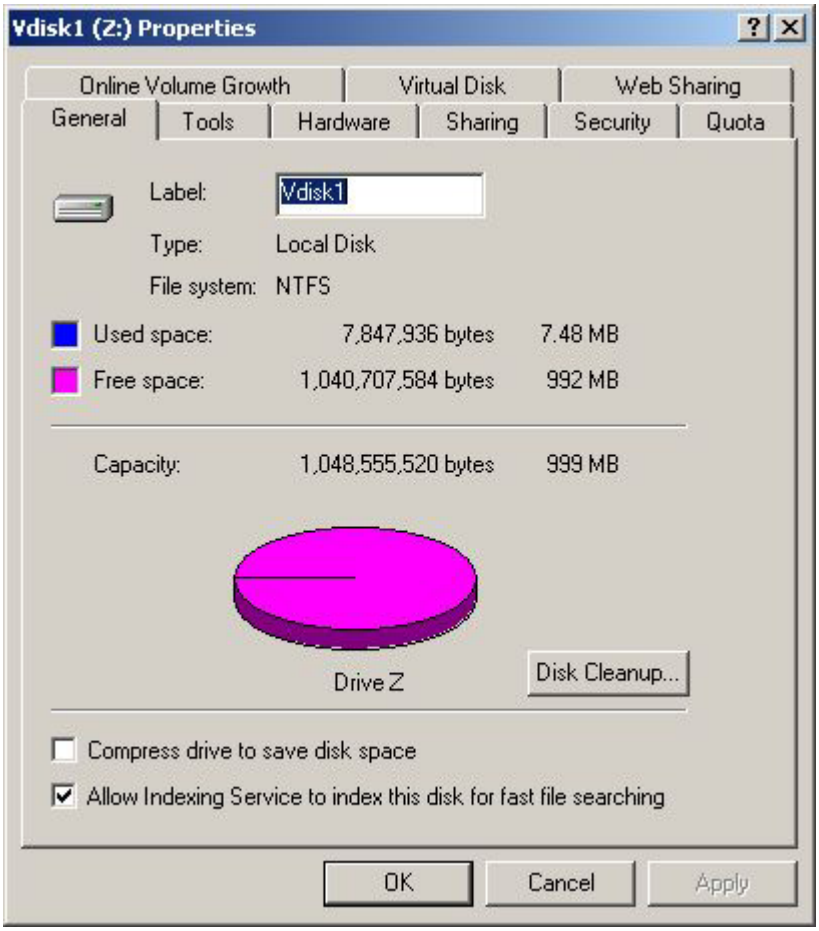


16. Right-click *Vdisk1* and select *Properties.*

    What is the amount of Delspace available?

    .....

17. Examine the information on each tab. Click *OK* when you are finished.
18. Minimize the MMC.



19. Using Windows Explorer (or My Computer), right-click *Vdisk1* and select *Properties* to examine the properties (General, Tools, Hardware, Quota, Sharing, Security, and Quota tabs).

    Note that it has the same attributes as a physical disk. Also note the additional tabs:

    - **Virtual Disk tab** — Provides information specific to the virtual disk.
    - **Online Volume Growth tab** — Allows you to dynamically expand the size of the virtual disk. Do **not** grow the volume at this time.

20. Click *OK* when you are finished.

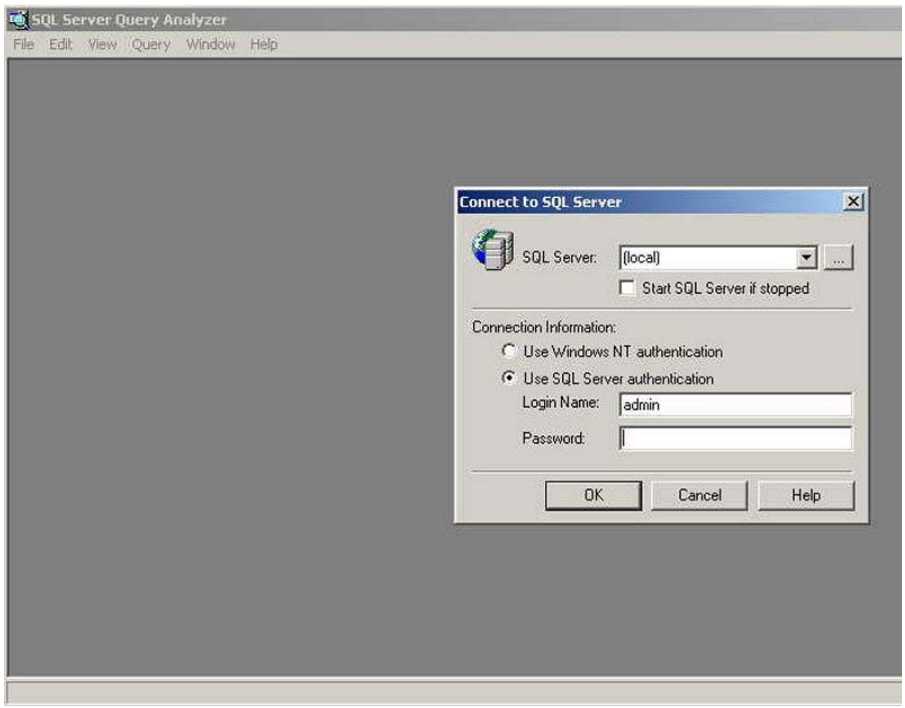
Section 2 — Using Snapshots for Data Recovery

Exercise 1: Application Startup

In a business environment, recovery actions result from data corruption or loss of application data in a database. In this exercise, you will start a simulated application and corrupt (delete) the data.

> **Note**
> If you do not have a c:\scripts directory, your instructor will point you to the files necessary to start this application data simulation.

1. Using Windows Explorer, find the batch file *CreateDB_VR.bat*. Double-click the *CreateDB_VR.bat* batch file to execute it.
2. Locate *iSQLw.exe* and double-click the file.



3. Log in with the admin user ID *admin* and no password. Use the defaults for any other parameters.
4. Select *File* → *Open* → *CreateOriginal_VR.sql.*

   The SQL statement in this query creates a simulation of data entry in a database application.
5. Click the green arrow (run) icon in the menu bar to execute the SQL script.
6. Move the *iSQLw.exe* window to the upper left corner of your screen so that it remains visible.

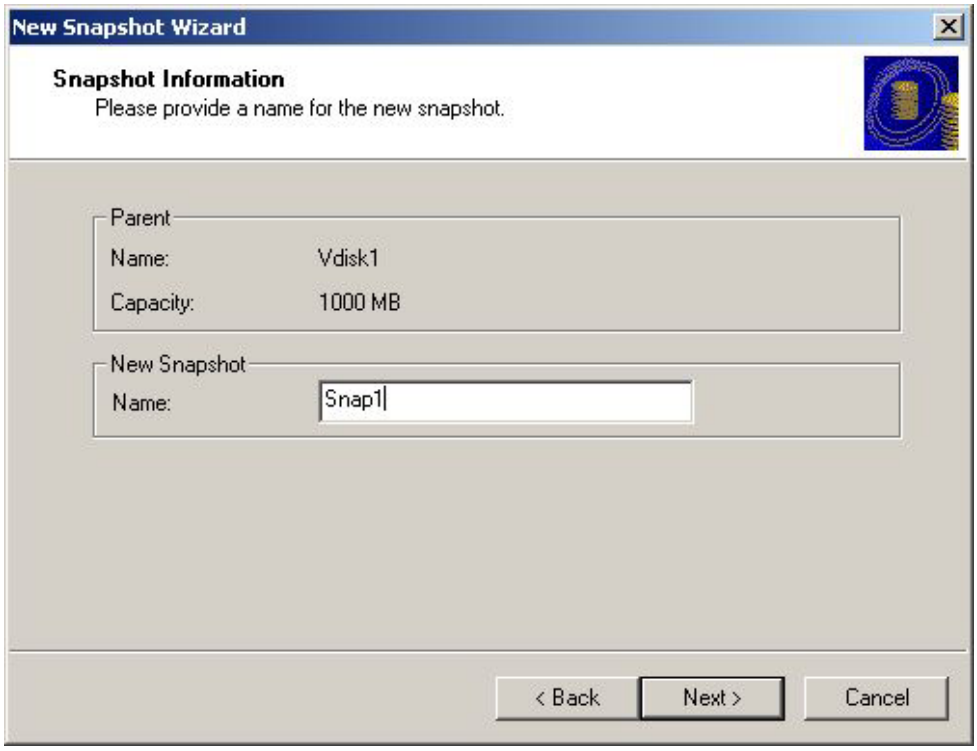
Exercise 2: Deleted File Recovery

To recover a file that was deleted from the production database:

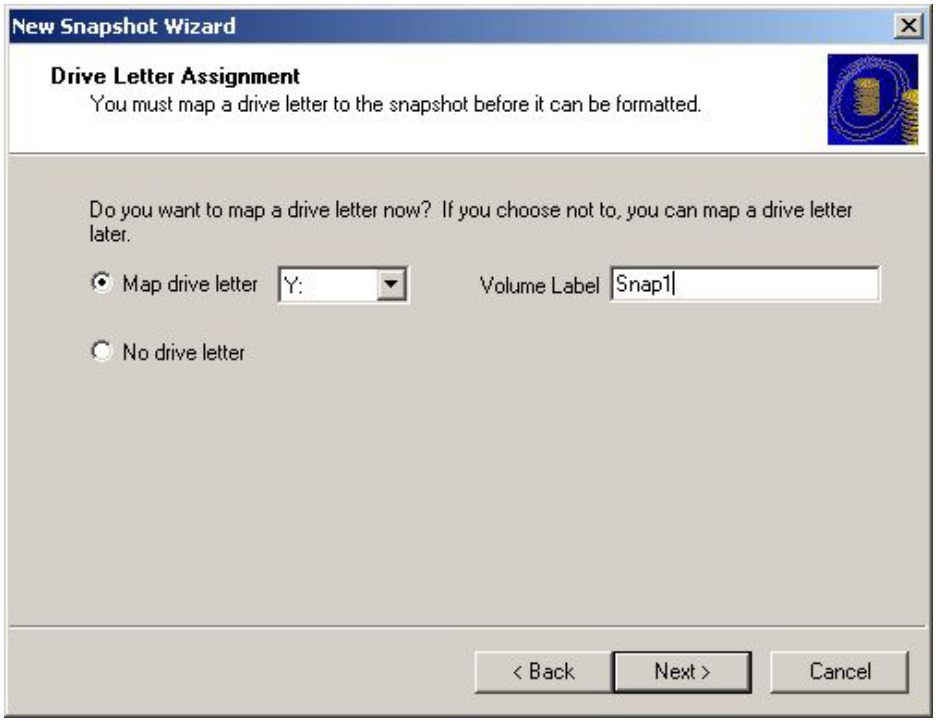
1. Double-click the SQL Server icon in your system tray to open the SQL Server manager.

2. Click *Pause* → *Yes* to pause the SQL Server application.
3. Open Snapshot Manager.
4. Expand *Pool1,* then right-click *Vdisk1*.
5. Select *New* → *Snapshot*.

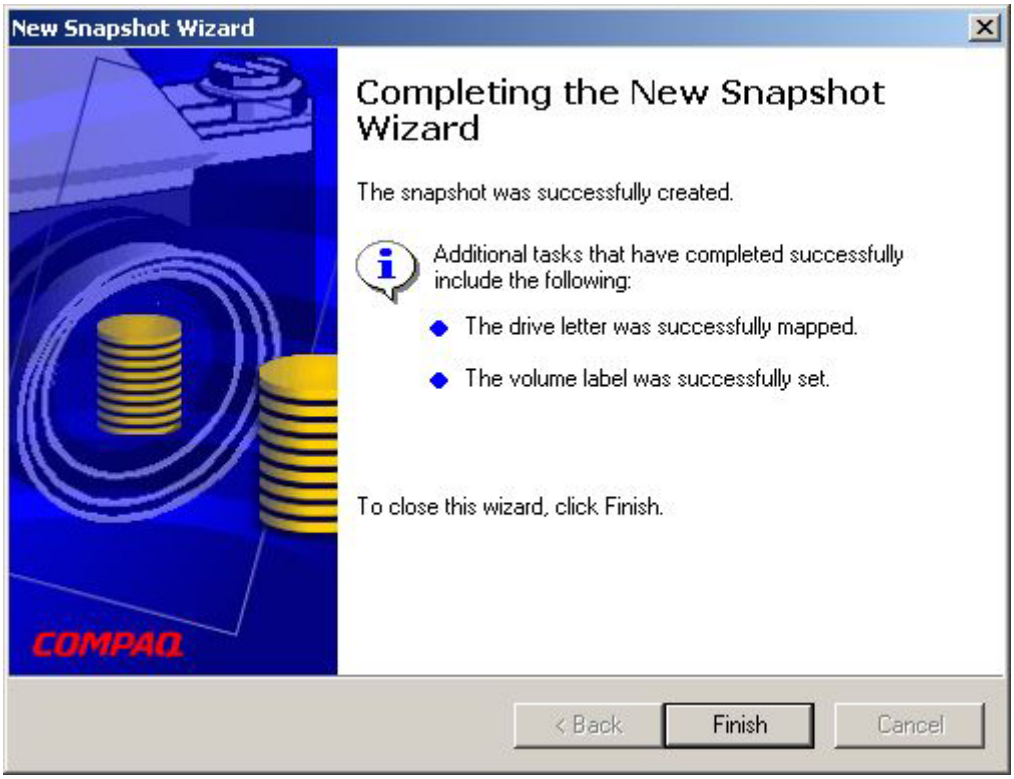
6. When the New Snapshot Wizard displays, click *Next*.



7. Enter *Snap1* as the New Snapshot Name, Click *Next*.



8. On the next screen, select *Map drive letter.* Select *Y:* from the drop-down list.
9. Change the Volume Label to *Snap1* (defaults to the volume label of the parent disk), then click *Next*.



10. When the completion window displays, click *Finish.*

    How long did it take to create the snapshot?

    .....

    What was the affect (if any) on the iSQLw.exe application?

    .....

11. Return to the SQL Server management window and click *Start/Continue* to restart the server.
12. Return to the iSQLw.exe window and click the red block (stop) icon in the menu bar to stop the query.
13. Using Windows Explorer, find the *PseudoApplicationDB_data.mdf* file in the \data directory on your virtual disk (Z:).

    What is the size of the data file? .....

14. Using Windows Explorer, find the *PseudoApplicationDB_data.mdf* file in the \data directory on your snapshot disk (Y:).

    What is the size of the data file? .....

15. Return to the SQL Server management window and click *Stop* → *Yes*.
16. Using Windows Explorer, delete the database file *z:\data\PseudoApplicationDB_data.ldf*.
17. Return to the SQL Server management window and click *Start/Continue*.
18. Return to the iSQLw.exe window and rerun the query (click the green arrow icon).

    What is the result?

    .....
19. Return to the SQL Server management window and click *Stop* → *Yes*.
20. Copy both database files from the snapshot (copy and paste).
21. Return to the SQL Server management window and click *Start/Continue*.
22. Return to the iSQLw.exe window. Select *File* → *Open* → *CreateOriginal_VR.sql*. Run the query (click the green arrow icon).

    What is the result?

    .....

Note

Another option for restoring data is Virtual Replicator Flashback, which restores the entire virtual disk from a snapshot.

Exercise 3: Damaged Disk

The purpose of this exercise is to simulate a disk failure in the pool:

1. At the iSQLw.exe window, select *File* → *Open* → *ShowData.sql*. Run the query (click the green arrow icon).

   What is the result?

   .....

2. At the storage system, physically remove all drives used in the virtual pool.

3. Using Windows Explorer, try to delete the database log file *z:\data\PseudoApplicationDB_log.ldf*.

   What is the result?

   .....

4. Return to the iSQLw.exe window and rerun the query (click the green arrow icon).

   What was the result?

   .....

5. Attempt to copy the deleted file from the snapshot drive (Y:).

   What is the result?

   .....

6. Replace the drives removed in step 3.

Section 3 — Online Volume Growth (Optional)

Overview

Virtual Replicator lets you increase storage capacity without disrupting operations on Windows 2000 systems. Typically, when you grow a RAIDset, the operating system does not recognize the change until you reboot. The Virtual Replicator Online Volume Growth feature directs the operating system to update the size of a physical or virtual disk without requiring a system restart.

There are two exercises in this section:

- Exercise 1: Growing a Virtual Disk
- Exercise 2: Adding Storage to the System, Expanding the Pool, and Growing the Virtual Disk

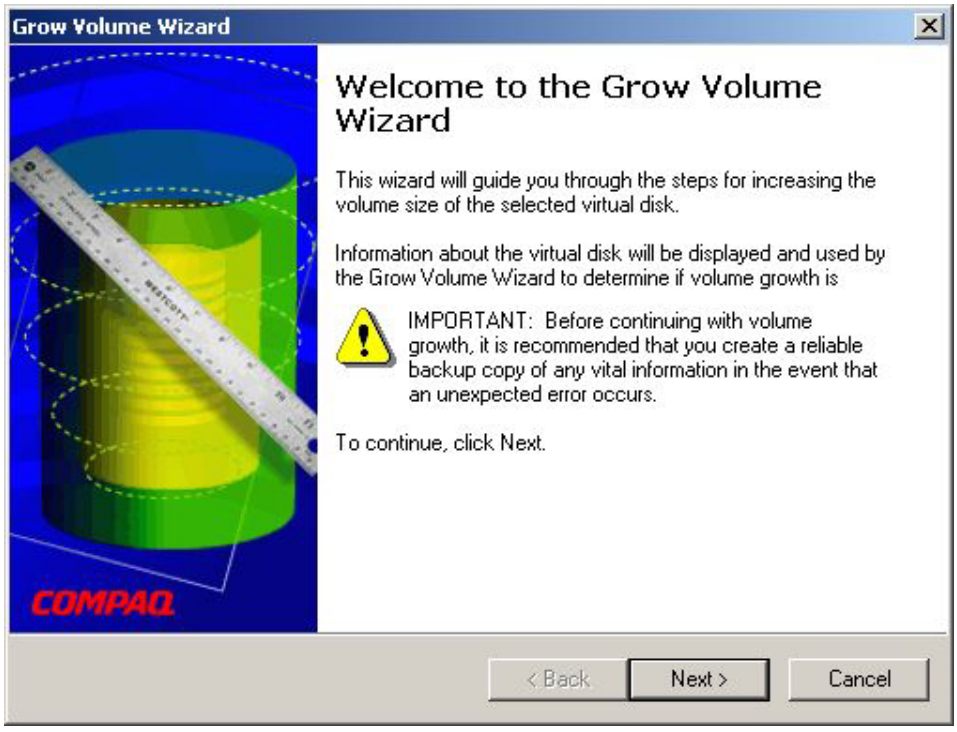
Exercise 1: Growing a Virtual Disk

To grow a virtual disk while the data remains online and accessible:

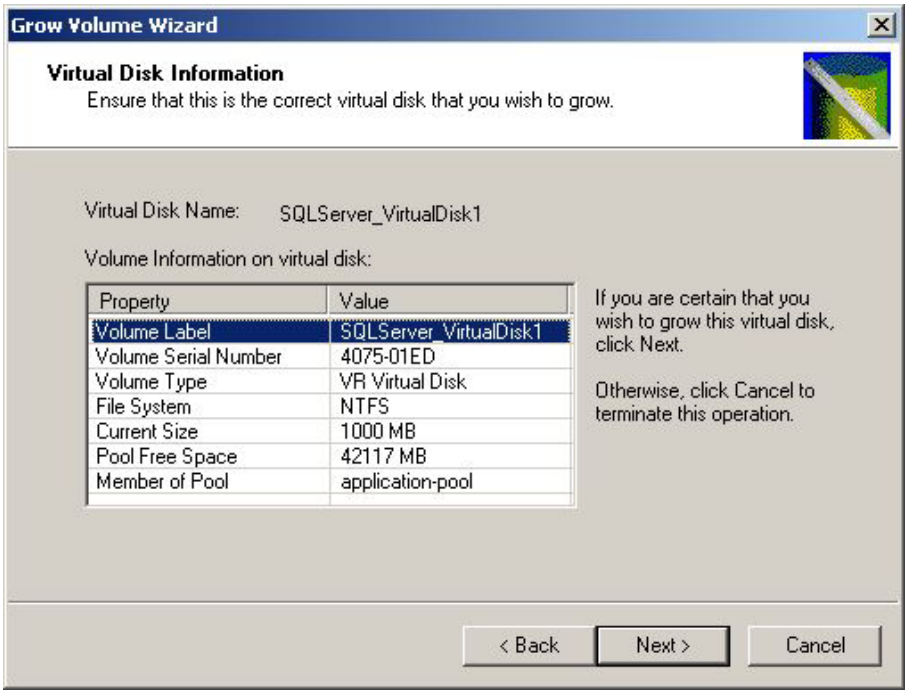
1. Return to the iSQLw.exe window. Select *File* → *Open* → *CreateOriginal_VR.sql* and accept the default login parameters. Run the query (click the green arrow icon).
2. Move the iSQLw.exe window up to the left of the screen.
3. Using Windows Explorer (or My Computer), select *Vdisk1*. Right-click and select *Properties.* Note the capacity of the Virtual Disk.
4. Open Snapshot Manager.
5. Expand the *Snapshot Manager (Local)* folder to display the pool and its virtual disks and snapshots.
6. Right-click *Vdisk1*.
7. Select *All Tasks* → *Grow Volume*.

   What other task options are available?

   .....



8. The Online Volume Growth Wizard displays. Click *Next*.

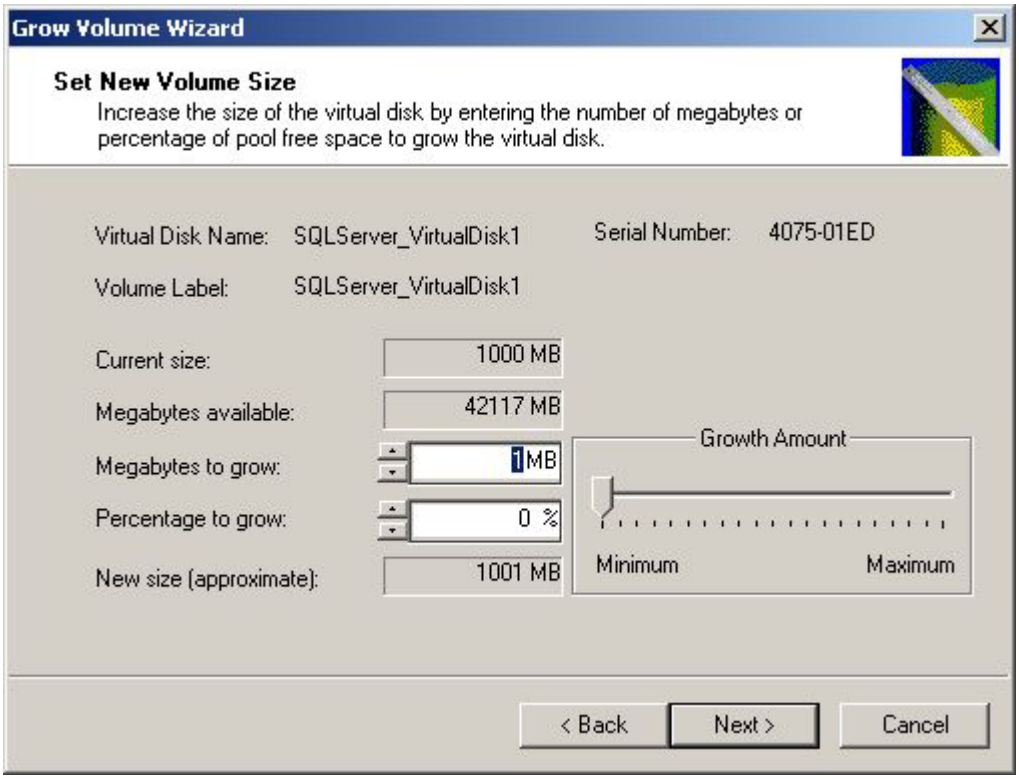


9. Current volume information about the virtual disk displays.

   What is the current size of the virtual disk and the available free space in the pool?

   .....

10. Click *Next*.



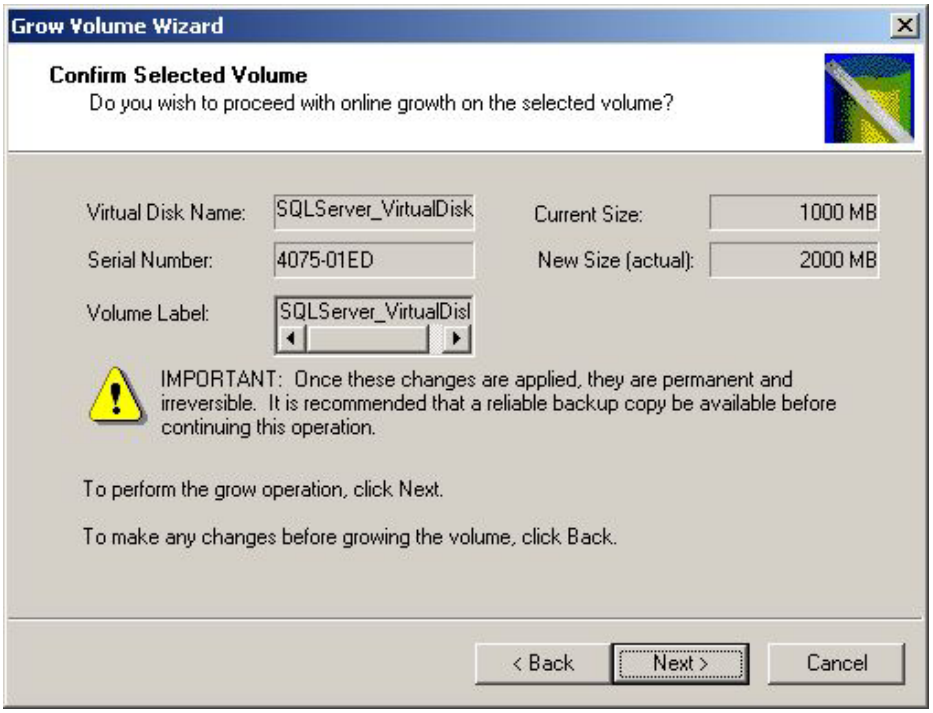
There are three methods for increasing the size of your virtual disk. You can enter the percent of available free space to add, use the Growth Amount slider, or enter the size in megabytes.

In the preceding graphics, to what amount can the virtual disk be expanded?

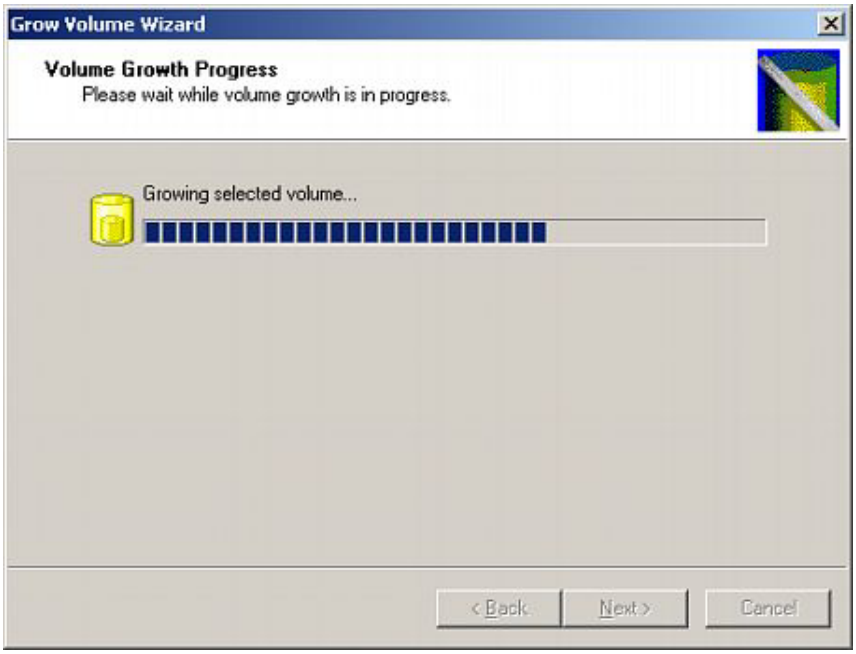
.....

(Hint: The limit to which the virtual disk may be expanded is the free space available in the pool.)

11. Increase the virtual disk by *1000MB* (1GB).
12. Click *Next*.



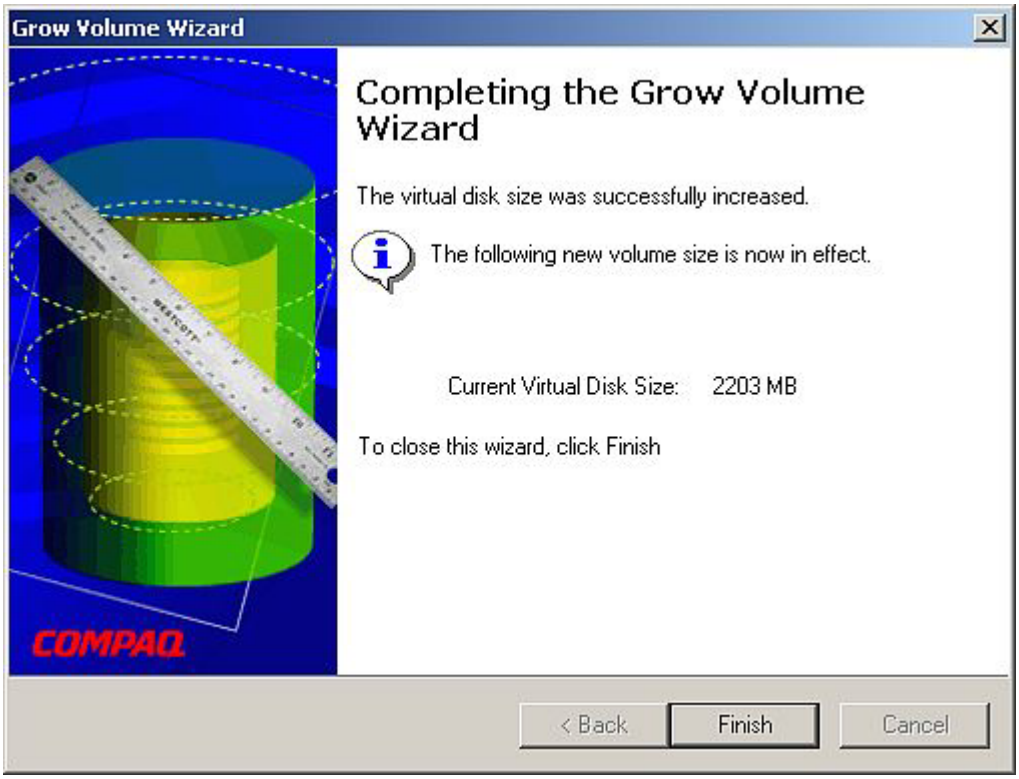
13. Click *Next* to confirm that you want to grow the selected volume.



The growth progress displays.

What is the effect (if any) on the iSQLw.exe application?

.....



14. Click *Finish*.

    Was the volume growth successful?

    .....

    If not, can you determine why?

    .....

15. Right-click *Snap1* and select *Delete* → *OK*.
16. Repeat steps 6 through 14.
17. Using Windows Explorer (or My Computer), select *Vdisk1*.
18. Right-click and select *Properties*.

    What is the new size of Vdisk1?

    .....

    What is the effect (if any) on the iSQLw.exe application?

    .....

19. Close the iSQLw.exe application. Select *No* to commit.

Exercise 2: Adding Storage to the System, Expanding the Pool, and Growing the Virtual Disk

This exercise shows how new storage is introduced to the system, added to the storage pool, and used to facilitate additional growth of a virtual disk.

1. Using Windows Explorer (or My Computer), copy *test.bat* from C:\Sample Data to *Vdisk1*.

   If *test.bat* is not available, you can recreate it using notepad to enter the following commands:

   ```
   @echo off
   :infinite
   xcopy "c:\program files" \  /E /Y
   goto infinite
   end
   ```

   Save the file as test.bat on your Vdisk1 drive.

2. Double-click *test.bat* to begin running the batch file.

   test.bat provides continuous activity to *Vdisk1* to simulate a running application.

3. Arrange the cmd.exe window so that it occupies the upper right corner of the screen. Leave it running.

3. Open Snapshot Manager.

4. Expand the *Snapshot Manager (Local)* folder to display the pool and its virtual disks and snapshots.

5. Right-click *Pool1* and select *Properties*. Click the *Storage Units* tab, the click *Add*.

   What is the result?

   .....

6. Introduce an additional disk drive (provided) into an empty bay in your storage system.

   Note
   Use the appropriate management utility (ACU or CLI) to create a LUN to present to the host.

7. Allow the new device to spin up.

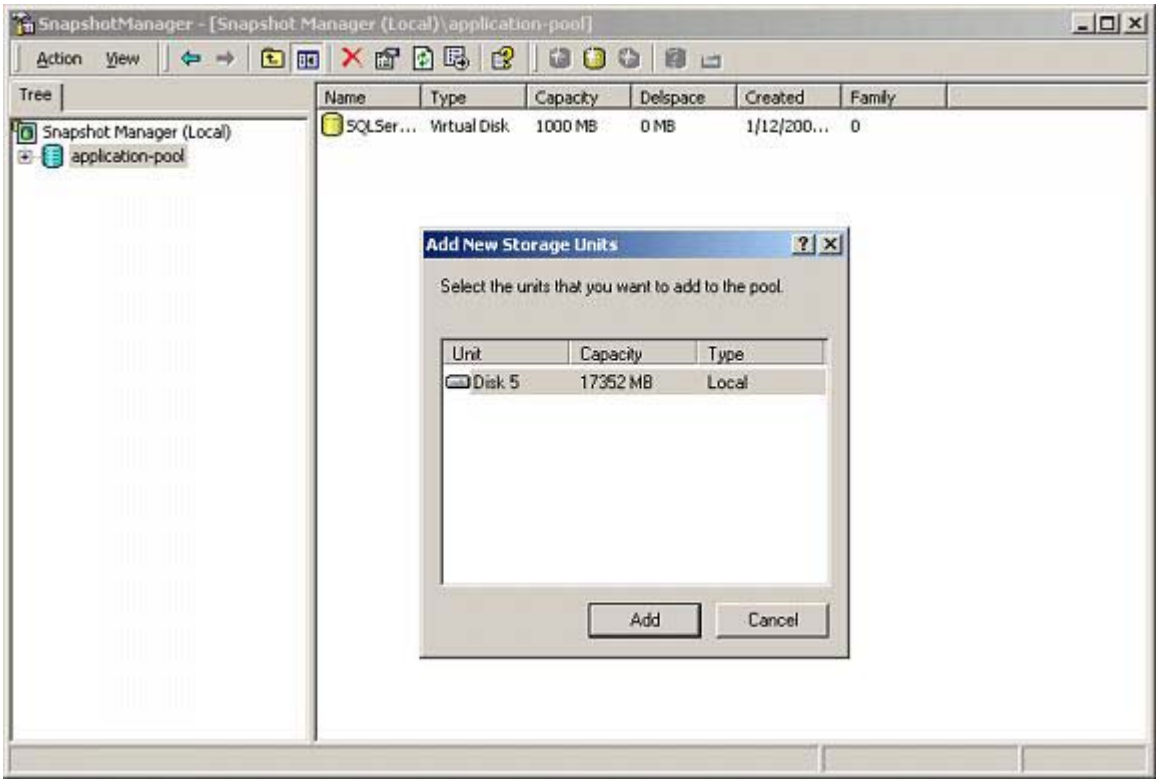
8. Right-click *My Computer* and select *Manage*.

9. Right-click *Disk Management* and select *Rescan Disks.*

10. If the new unit displays as a dynamic disk, right-click the new unit and select *Revert to Basic Disk*.
11. Close the Computer Management window.
12. Open Snapshot Manager.
13. Right-click *Pool1* and select *Properties*.
14. Click the *Storage Units* tab.
15. Click *Add*.

Note

You can also right-click *Pool1* and select *All Tasks* → *Add Unit*.

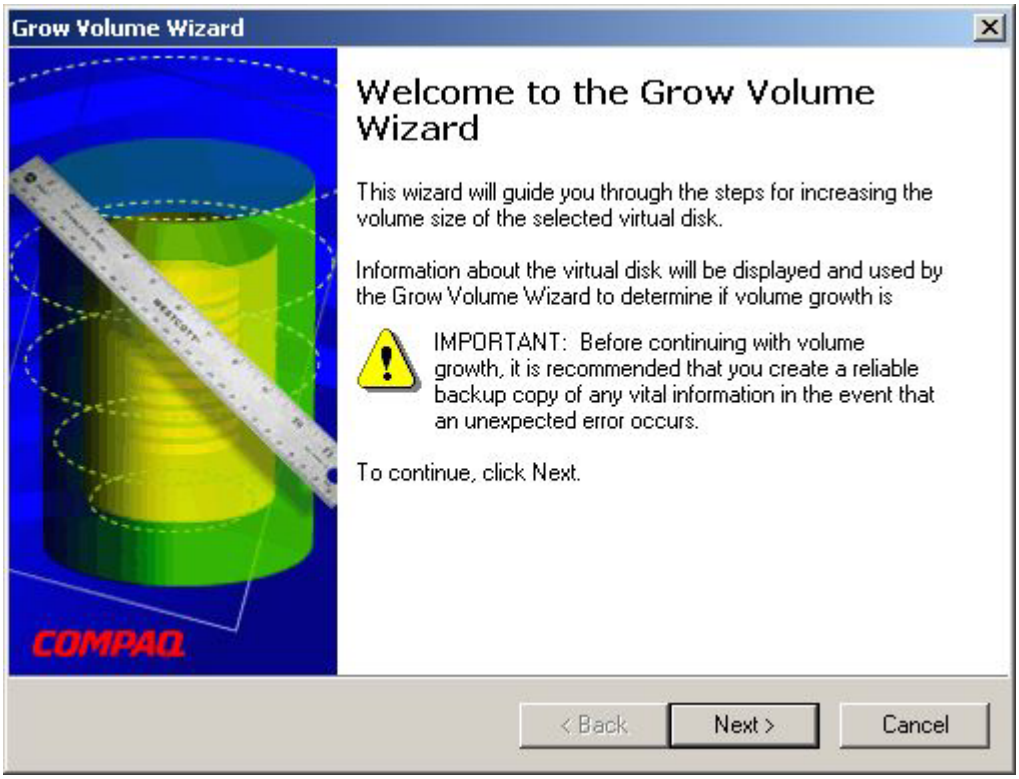


16. Click *Add* to add the new storage device to the pool.

    What is the effect (if any) on the copy operation?

    .....

17. Click *OK*.
18. Right-click *Vdisk1*. Select *All Tasks* → *Grow Volume*.

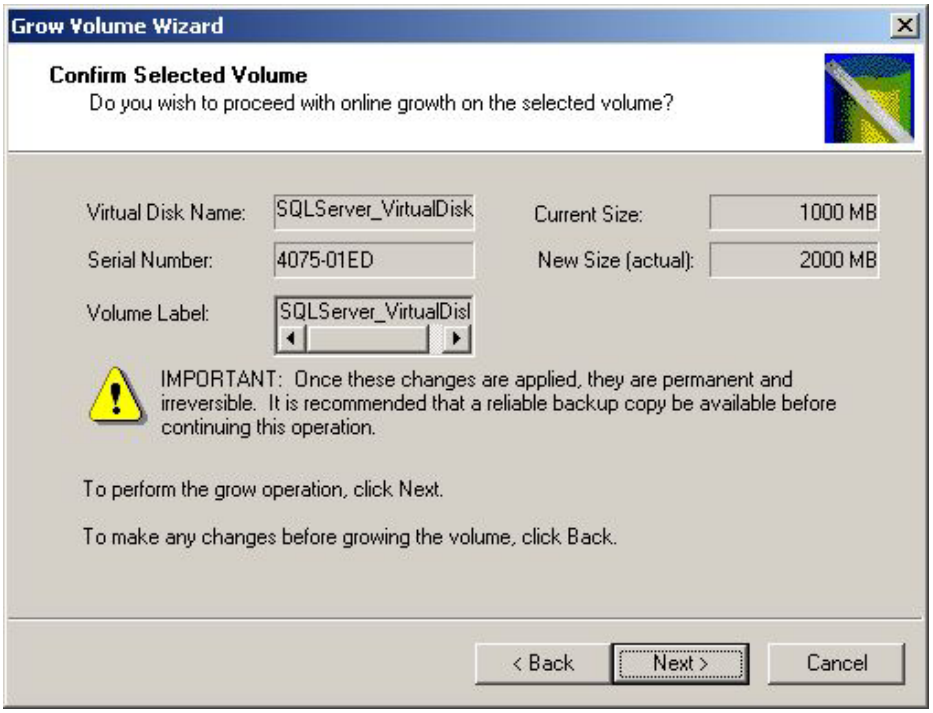


19. The Online Volume Growth Wizard displays. Click *Next*.
20. Information about the Virtual Disk displays.

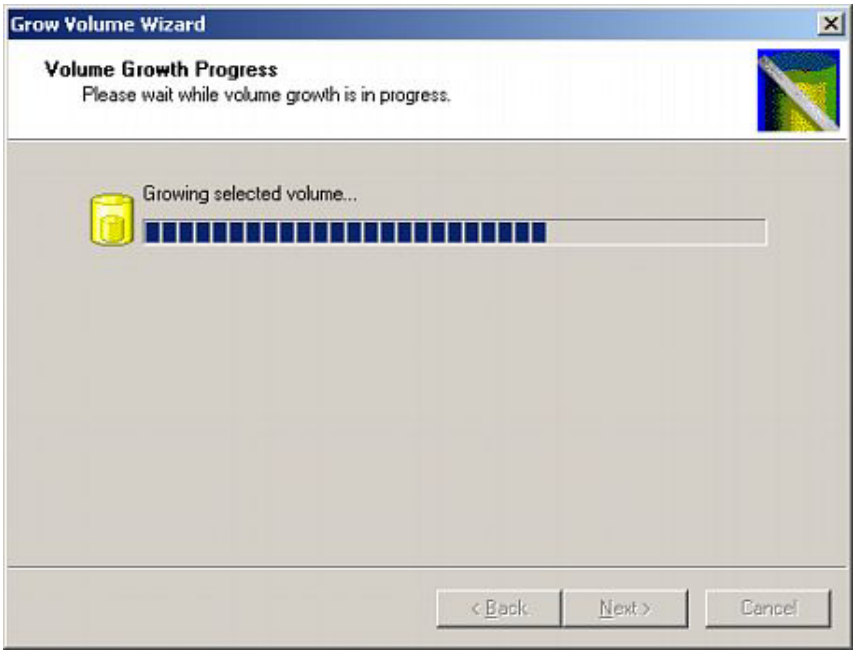
    What is the current size of the Virtual Disk and the available free space in the pool?

    .....
21. Click *Next*.

    The limit to which the Virtual Disk may be expanded is the free space available in the pool.
22. Increase the virtual disk by *2000MB* (2GB).
23. Click *Next*.



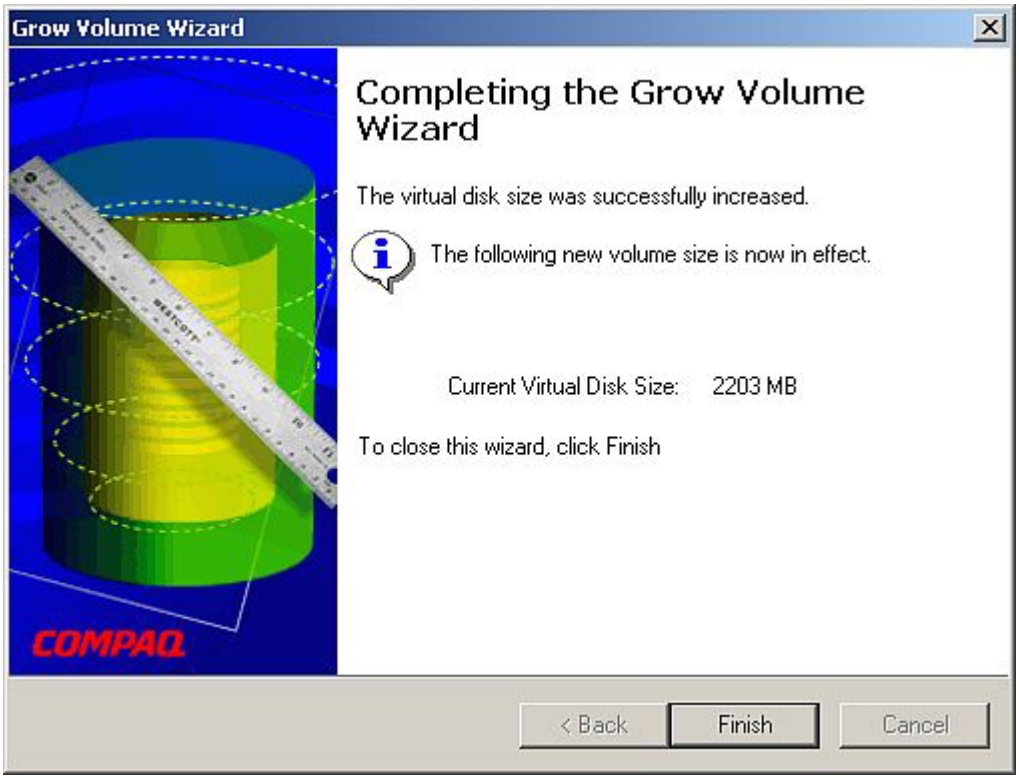
24. Click *Next* to confirm that you want to grow the selected volume.



The growth progress displays.

What is the effect (if any) on the copy operation?

.....



25. Click *Finish*.
26. Using Windows Explorer (or My Computer), select *Vdisk1*. Right-click and select *Properties*.

    What is the new capacity of the virtual disk?

    .....
27. Stop the *test.bat* batch file.

Section 4 — Deleting Virtual Disks, Snapshots, and Pools

Overview

In a normal business environment, a pool would not be deleted. The deletion of all snapshots, virtual disks, and the pool are included here to give you experience in the procedure.

There is one exercise in this section.

Exercise 1: Deleting Virtual Disks, Snapshots, and Pools

To maintain optimum system performance, avoid keeping snapshots for long periods of time if the data changes frequently.

When data on a parent disk changes, segments are copied-out to each snapshot of the parent disk. Virtual Replicator keeps track of copy-outs by associating an address with each segment of data. During startup, Virtual Replicator pools "rebind" by re-establishing these address connections. The rebinding process is usually quick, but can take much longer if you have a lot of snapshots containing large amounts of changed data (copy-outs).

> **Note**
> Virtual Replicator provides a utility, called SmartSnap, that can automate the number of snapshots maintained for a virtual disk. SmartSnap can be invoked from the command line.

Virtual Replicator should not be considered your only means of backup. It is recommended that you use Virtual Replicator in conjunction with a standard backup tool.

To delete a pool and its contents.

1. Open Snapshot Manager.
2. Right-click *Pool1*.
3. Select *Delete*.

   Were you able to delete the pool? .....

   What message displays?

   .....
4. Right-click *Vdisk1*.

5. Select *Delete*.

   Were you able to delete the virtual disk? .....

   What message displays?

   .....

6. Right-click *Vdisk1*.
7. Select *Delete*.

   Were you able to delete the virtual disk? .....

8. Right-click *Pool1*.
9. Select *Delete*.

   Were you able to delete the pool? .....

   What message displays?

   .....

10. Close Snapshot Manager.
11. Uninstall Virtual Replicator from the host.

Objectives

Your customer, Widget Inc., was impressed by the added functionality HP OpenView Storage Virtual Replicator provided for their backup needs, but was interested in an Enterprise solution for their data storage, rather than a host-based software product. They were also concerned about the failure of the pool when they had a disk failure.

Widget would like to create clones of their data. They would also like the ability to mount the clone to their application server for quick restores. They would like you to demonstrate the abilities of the HP StorageWorks Enterprise Volume Manager (EVM) using a sample database.

After completing this lab, you should be able to:

- Create a job that performs a snapshot operation and automatically mount the snapshot on a host.
- Recover a lost or damaged file from the snapshot
- Create a job that performs a clone operation, splits the clone from the original, and mounts the clone on a host.
- Recover lost or damaged data from a disk failure.

Prerequisites

- Microsoft Windows 2000 Server installed on one computer which will serve as the host.
  - Service Pack 2 installed.
  - MSIE 5.50 or greater installed.
  - EVM host agent installed.
- EVM 2.0 D server installed on the OpenView SAN Management Appliance.
- RA8000/MA8000 storage configured as follows:
  - A LUN assigned to D1. D1 consists of two mirrored drives.
  - D1 is identified by the Windows 2000 host, formatted as NTFS, and assigned drive letter Z.
  - One drive recognized by the controller and not yet assigned to any LUN.
  - The script directory *c:\scripts* is on local drive C of the EVM host and is to be used in application simulation.
  - In *Settings* → *Control Panel* → *System*, click the *Advanced* tab, click *Environment Variables*, double-click the path variable and add *;c:\scripts* to the end of the string.

! Important

Versions prior to EVM 2.0 D and Secure Path 4.0 do not support Windows 2000 Dynamic Disks. BCVs can be created from source units configured as Dynamic disks, but attempting to mount these BCVs will result in a job failure.

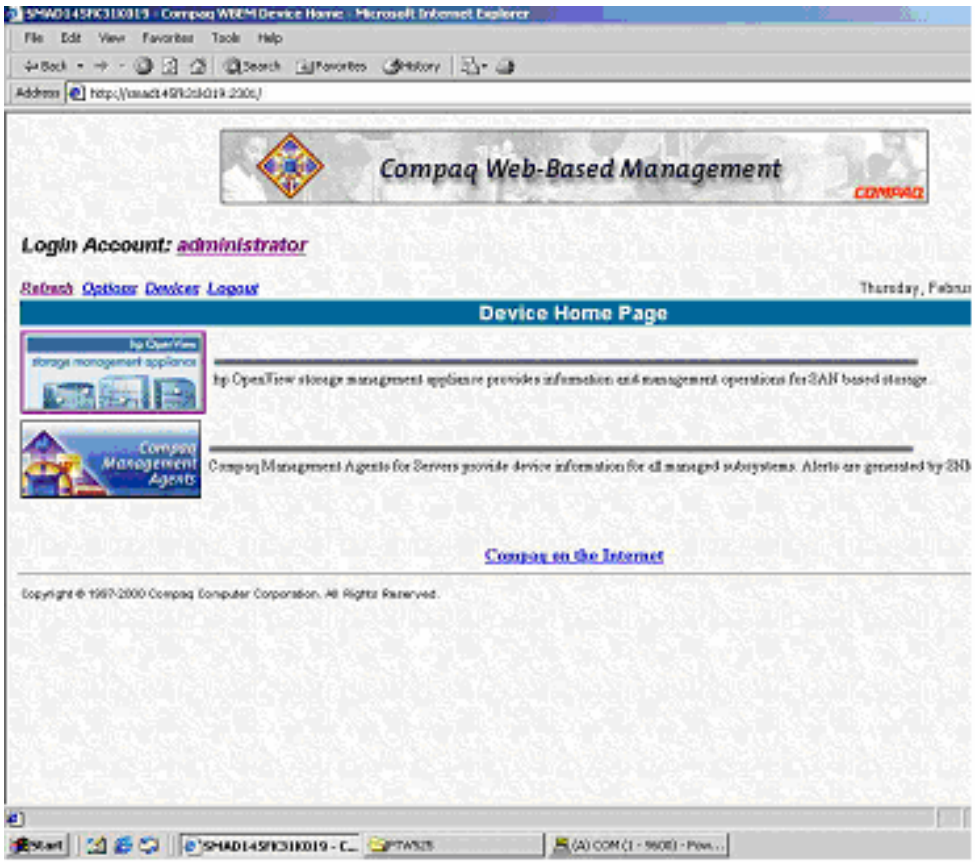
If the EVM host agent software is installed on a computer containing dynamic disks, the EVM Resources page for that computer displays two icons for each dynamic disk. One icon shows the drive letter of the device with no physical device information. The second icon shows an unmounted physical device with no drive letter.

Exercise 1 — Snapshot

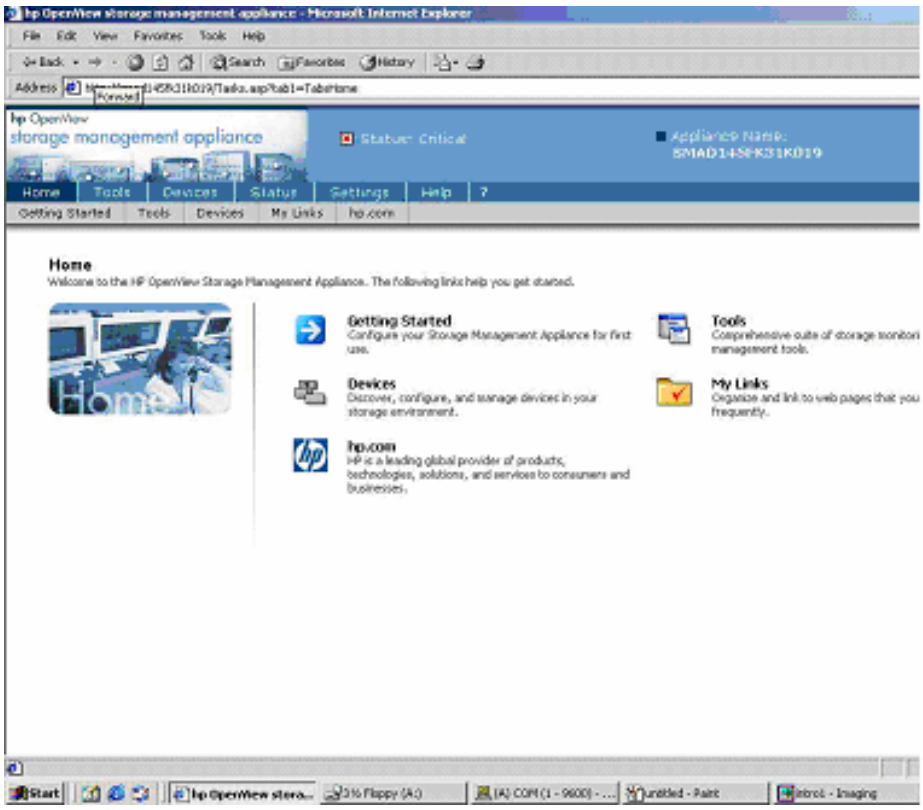
In a typical business environment, an EVM job would create a snapshot after quiescing any running applications, restart the application, mount the snapshot on the backup server, and then initiate the backup. In the interest of time, this exercise performs the quiesce, snapshot, restart, and mount procedures, but does not initiate a backup.

1. Browse to the Management Appliance using http://*appliancename*:2301.

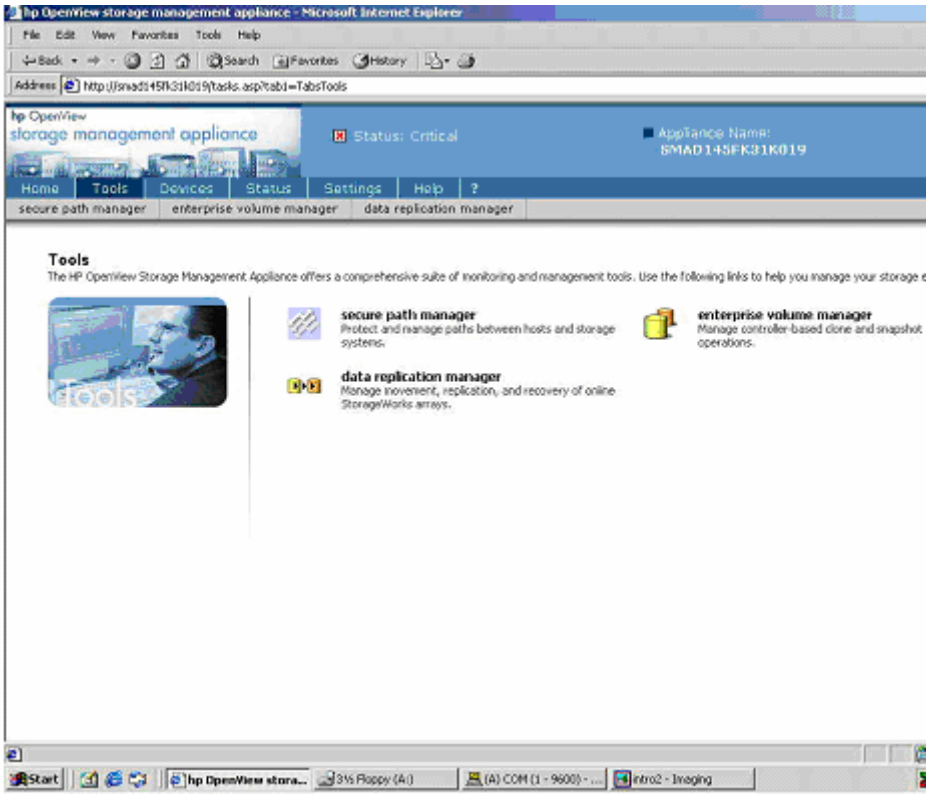
2. Log in with the password and user ID *administrator/administrator*.
3. Click *OK*.



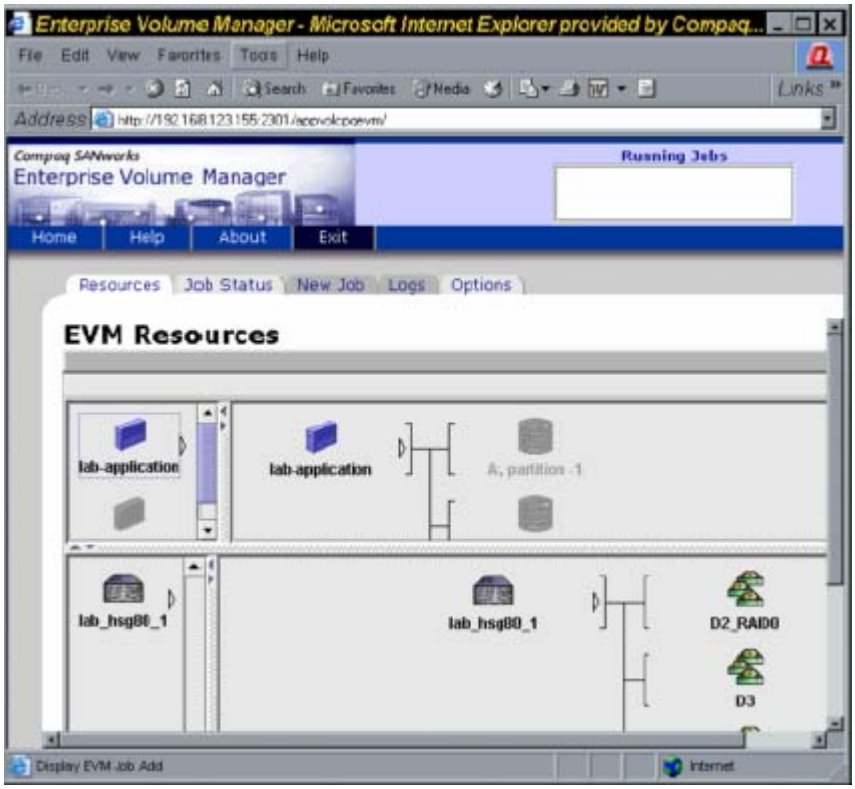
4. Click on the hp OpenView Storage Management Appliance button and when the below dialogue box appears login with the User Name of *administrator* and the password of *adminXXXXXX* (where XXXXXX is the last six digits of the Storage Management Appliance's serial number reversed—CASE SENSITVE---Letters will always be in UPPER case).



5. Click on the Tools button.



6. Click on the Enterprise Volume Manager button.



! Important

If your storage system is grayed out, launch HSG Element Manager and verify that the storage system is enabled. If it is disabled:

1. Select the *Enable* radio button.
2. Click *Submit.*
3. Close the browser and re-launch HSG Element Manager to ensure that the controllers are now visible.
4. Launch *Appliance Manager.*
5. Click *Services.*
6. Restart the Enterprise Volume Manager service.

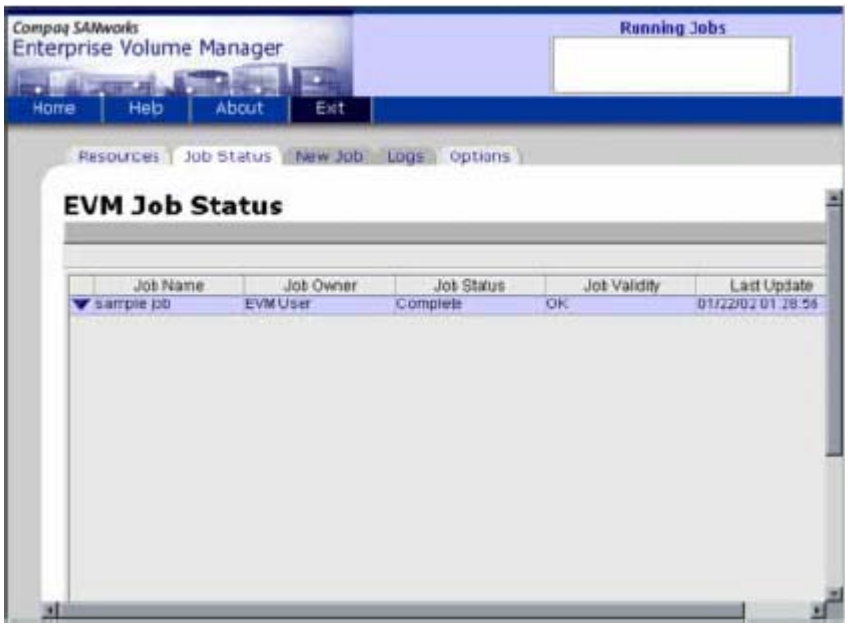
7. Click a storage subsystem (lower pane) to display the units and hosts associated with that storage unit.
8. Click a host (upper pane) to display the drives in use on that host.

Note

Right-click the icon for your storage unit and verify that an ACS firmware version is displayed. If there is no firmware version, the storage, switch, and appliance might not have been brought up in the correct sequence. Close the Enterprise Volume Manager window. Restart the Enterprise Volume Manager service using the steps 4 through 6 in the "Important" statement after step 7.

If you are still unable to see the firmware version, restart the Appliance and launch Enterprise Volume Manager again.

9. Select the *Job Status* tab.

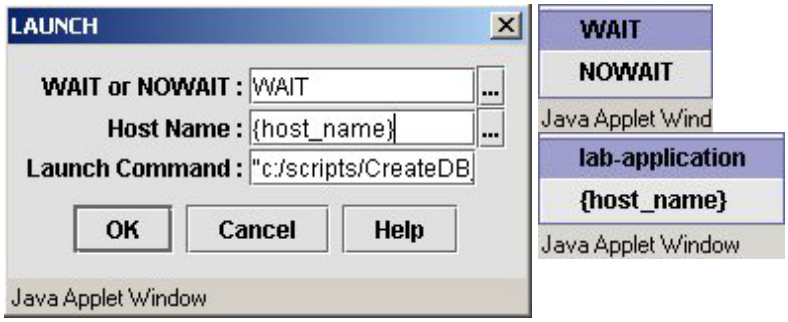


10. Right-click *sample job* and select *View job details*.
11. Click *Exit* to return to the Job Status window.
12. Right-click *sample job* and select *Execute*.
13. Select the *Logs* tab. Double-click the text file associated with the sample job (job_sample job_1.txt) and view the list of steps from the sample job.
14. Close the text view window.

15. Select the *New Job* tab.

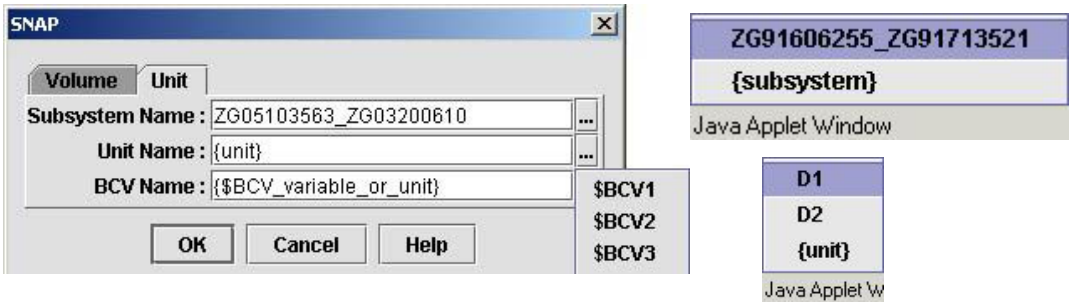
> **Note**
> At this time, you have the option to choose a job template or select commands. For these exercises you will select each command individually. You can add comments using the ";" command.

16. Double-click *LAUNCH* twice so that two batches will be launched.
17. Double-click *SUSPEND* to suspend SQL Server.
18. Double-click *SNAP* to create the snapshot.
19. Double-click *RESUME* to restart SQL Server.
20. Double-click *MOUNT* to mount to the host.
21. Double-click *LAUNCH* to launch a pseudo backup application.
22. Enter *SnapshotXX* as the Job Name (where *XX* is your class station number).

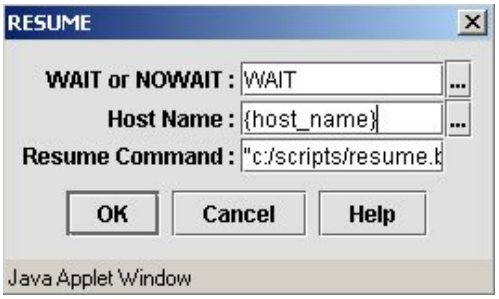


23. Double-click the first occurrence of the *LAUNCH* entry under Step/Sequence.
24. Click the ellipsis (…) beside Host Name to display the available hosts, then select the host on which the batch will be run.
25. In the Launch Command field, enter *"c:/scripts/CreateDB_EVM.bat"*.
26. Double-click the second occurrence of the *LAUNCH* entry under Step/Sequence.
27. Click the ellipsis (…) beside WAIT or NOWAIT to display the available options. Select *NOWAIT*.
28. Click the ellipsis (…) beside Host Name to display the available hosts, then select the host on which the batch will be run.
29. In the Launch Command field, enter *"c:/scripts/InsertOriginal_EVM.bat"*.

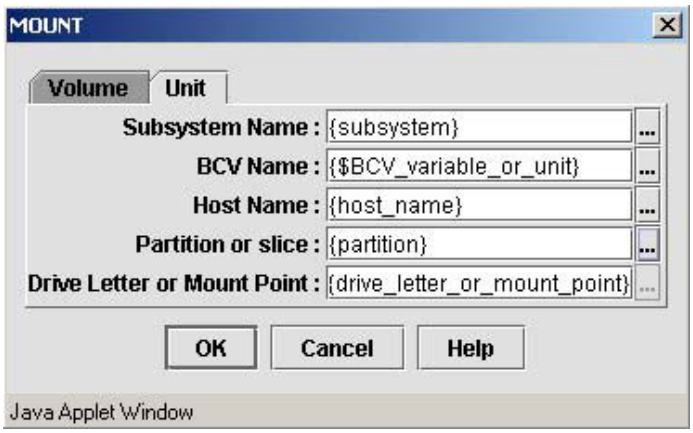
30. Double-click the *SUSPEND* entry under Step/Sequence.
31. Click the ellipsis (…) beside WAIT or NOWAIT to display the available options. Select *NOWAIT*.
32. Click the ellipsis (…) beside Host Name to display the available host, then select the host on which SQL Server is running.
33. Enter "*c:/scripts/suspend.bat"* in the Suspend Command field.
34. Double-click the *SNAP* entry under Step/Sequence.

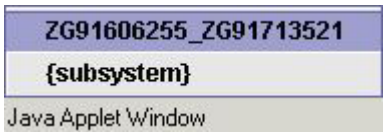


35. Select the *Unit* tab.
36. Click the ellipsis (…) beside Subsystem Name to display the available subsystems and select an available subsystem.
37. Click the ellipsis (…) beside Unit Name to display the units available on that subsystem and select an available unit.
38. Click the ellipsis (…) beside BCV Name. Select *$BCV1*.
39. Click *OK*.

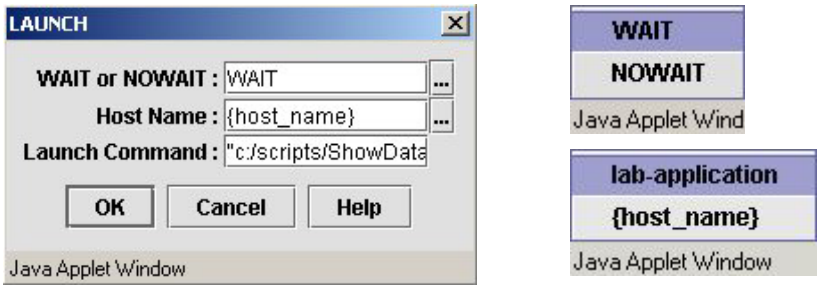


40. Double-click the *RESUME* entry under Step/Sequence.
41. Click the ellipsis (…) beside WAIT or NOWAIT to display the available options. Select *NOWAIT*.
42. Click the ellipsis (…) beside Host Name to display the available host, select the host on which SQL Server is running.
43. Enter *"c:/scripts/resume.bat"* in the Resume Command field.

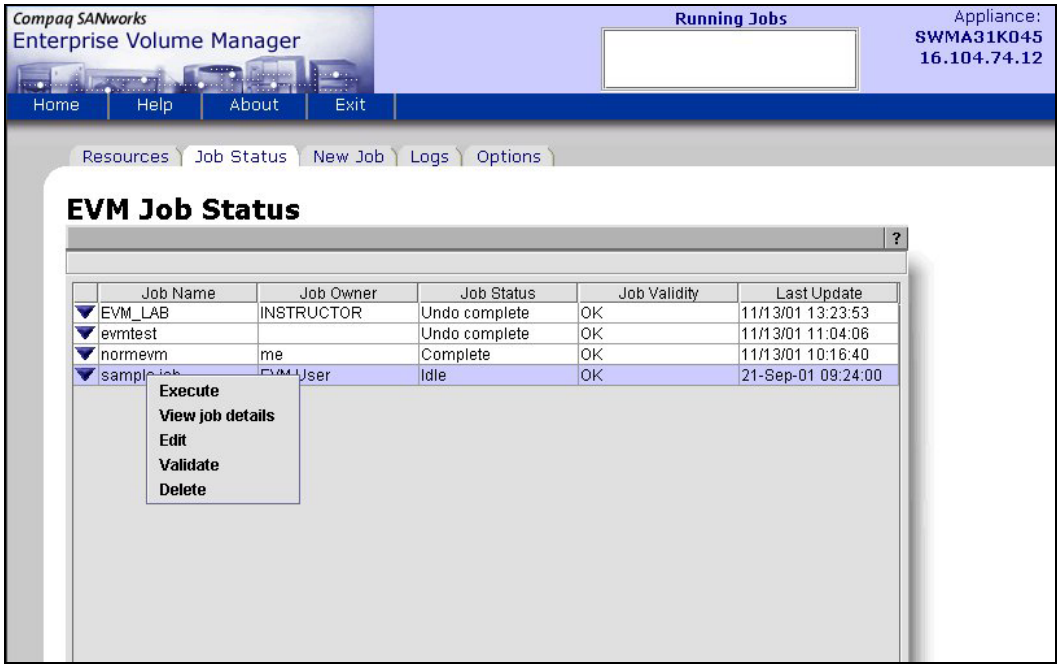




44. Double-click the *MOUNT* entry under Step/Sequence.
45. Select the *Unit* tab.
46. Click the ellipsis (…) beside Subsystem Name to display the available subsystems and select the same subsystem as you selected in the SNAP parameters.
47. Click the ellipsis (…) beside BCV Name and select the same variable name you entered for the SNAP command.
48. Click the ellipsis (…) beside Host Name to display the available hosts and select the one that is designated as your backup server.
49. Click the ellipsis (…) beside Partition or slice to display the options available and select an available partition. Enter *1*.
50. Enter *X:* as the Drive Letter or Mount Point.
51. Click *OK*.



52. Double-click last occurrence of the *LAUNCH* entry under Step/Sequence.
53. Click the ellipsis (…) beside WAIT or NOWAIT to display the available options. Select *NOWAIT*.
54. Click the ellipsis (…) beside Host Name to display the available hosts, then select the host on which the batch will be run.
55. In the Launch Command field, enter *"c:/scripts/ShowData.bat"*.
56. Click *Save* → *Exit* at the bottom of the New Job page.
57. Select the *Job Status* tab.



What is the Job Validity status of SnapshotXX (Where XX is your class station number)?

.....

58. Right-click on *SnapshotXX* (where *XX* is your class station number) and select *Validate*.

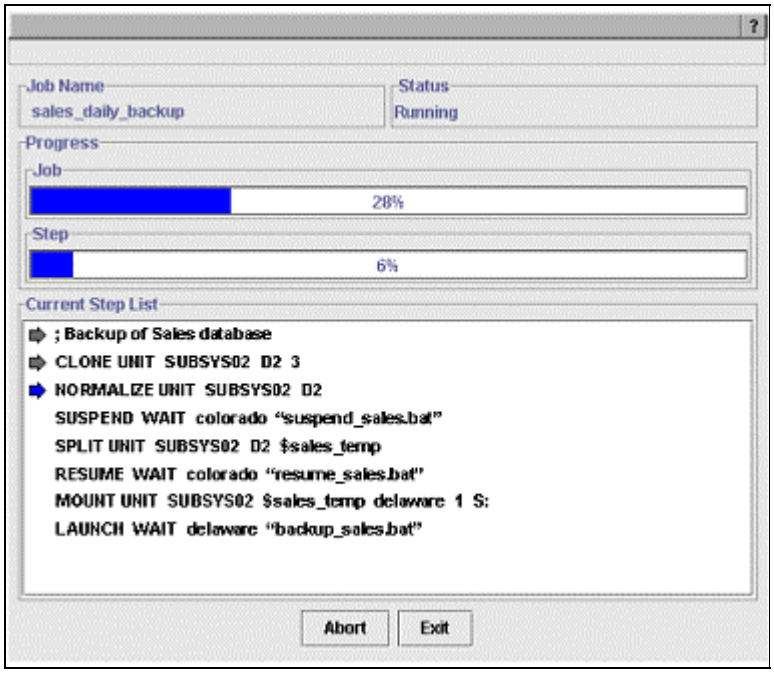
What is the Job Validity status of SnapshotXX (Where XX is your class station number)?

.....

59. Right-click *SnapshotXX* (where *XX* is your class station number) and select *Execute*.

> **Note**
> Although an EVM job does not have to be executed from the EVM host, for the purposes of this lab assume that the browser access to the Management Appliance and the EVM host is on the same server.

60. Right-click *SnapshotXX* (where *XX* is your class station number) and select *Monitor* to view the job in progress.



61. Double-click the SQL Server icon in your system tray to view status as the EVM job executes.

    Note what you observe at each of the job steps.

    First launch:.....

    Second launch: .....

    Suspend: .....

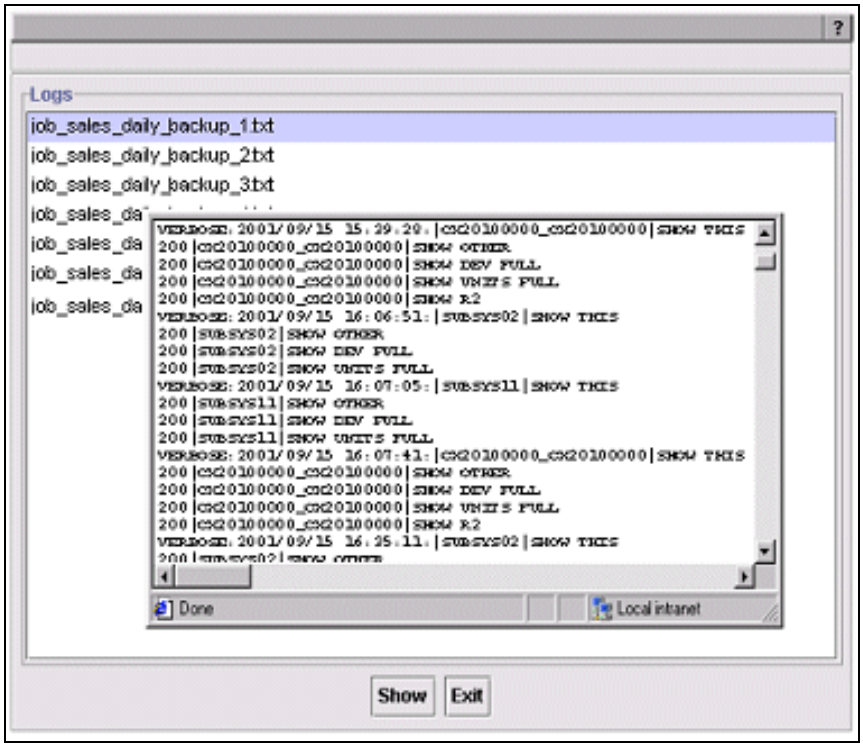
    Snap:.....

    Resume:.....

    Mount: .....

    Last launch: .....

62. When the job is complete, click the *Job Status* tab to return to the list of available jobs.



63. Select the *Logs* tab, then double-click the first text file for your job (for example, job_SnapshotXX_1.txt) and view the list of commands that were executed when the job was run.
64. On your backup server, right-click *My Computer* and select *Manage*.
65. Right-click *Storage* → *Disk Management* and select *Rescan*.
66. Verify that disk X: is mounted on that server.

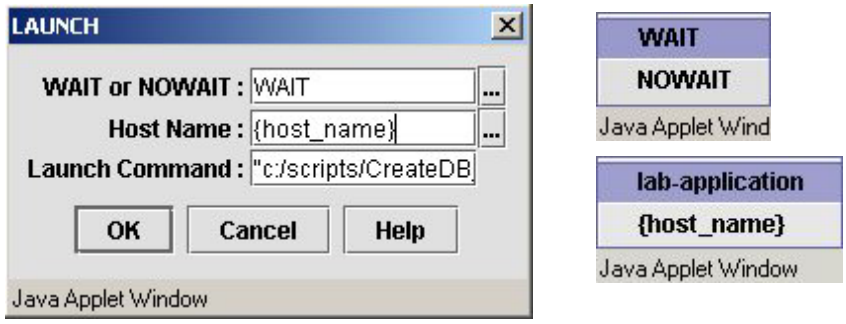
Exercise 2 — Managing a Clone

In a typical business environment, an EVM job would create a clone after quiescing any running applications, restart the application, split the clone off from the original mirrorset, then mount clone on the data-mining application or backup server.

67. Select the *New Job* tab.
68. Double-click *LAUNCH* twice so that two processes will be launched.
69. Double-click *SUSPEND* to suspend SQL Server.
70. Double-click *CLONE* to create a clone.
71. Double-click *NORMALIZE* to allow the clone to normalize.
72. Double-click *SPLIT* to split off clone.
73. Double-click *RESUME* to restart SQL Server.
74. Double-click *MOUNT* to mount to the host.
75. Double-click *LAUNCH* to launch a pseudo data mining application.

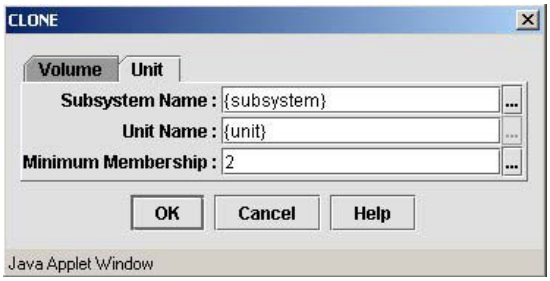
> **!** **Important**
> The CLONE command with less than a three-member mirrorset requires the NORMALIZE command to be included before the SPLIT command to allow the clone to normalize.

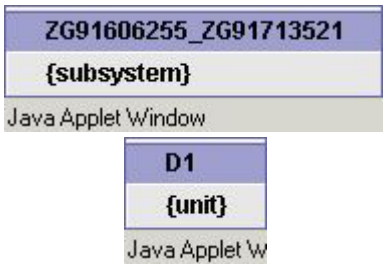
76. Enter *CloneXX* as the Job Name (where *XX* is your class station number).



77. Double-click the first occurrence of the *LAUNCH* entry under Step/Sequence.
78. Click the ellipsis (…) beside WAIT or NOWAIT to display the available options. Select *NOWAIT*.
79. Click the ellipsis (…) beside Host Name to display the available hosts, then select the host on which the batch will be run.
80. In the Launch Command field, enter "*c:/scripts/CreateDB_EVM.bat"*.
81. Double-click the second occurrence of the *LAUNCH* entry under Step/Sequence.
82. Click the ellipsis (…) beside WAIT or NOWAIT to display the available options. Select *NOWAIT*.
83. Click the ellipsis (…) beside Host Name to display the available hosts, then select the host on which the batch will be run.
84. In the Launch Command field, enter *"c:/scripts/InsertOriginal_EVM.bat"*.

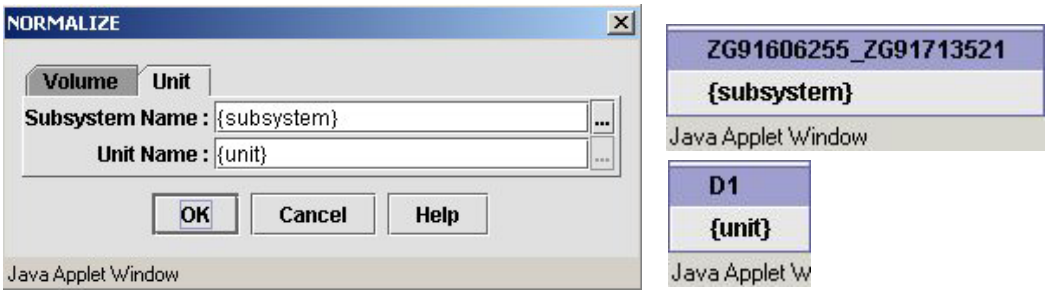
85. Double-click the *SUSPEND* entry under Step/Sequence
86. Click the ellipsis (…) beside WAIT or NOWAIT to display the available options. Select *NOWAIT*.
87. Click the ellipsis (…) beside Host Name to display the available host, then select the host on which SQL Server is running.
88. Enter *"c:/scripts/suspend.bat"* in the Suspend Command field.
89. Double-click the *CLONE* entry under Step/Sequence.



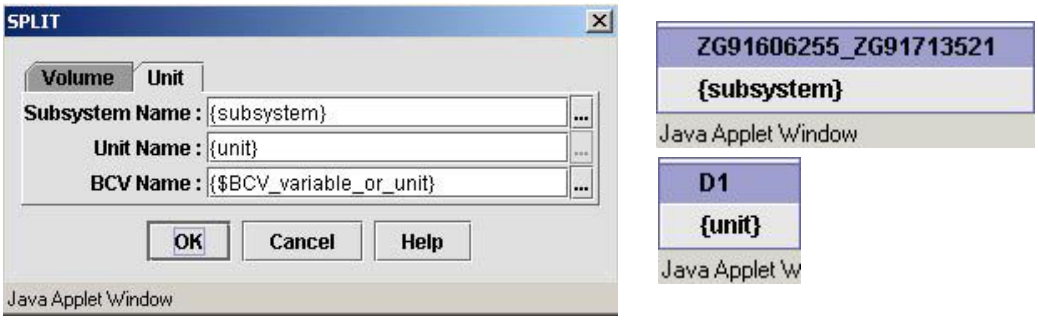


90. Select the Unit tab.
91. Click the ellipsis (…) beside Subsystem Name to display the available subsystems, then select an available subsystem.
92. Click the ellipsis (…) beside Unit Name to display the units available on that subsystem, then select an available unit.
93. Click the ellipsis (…) beside Minimum Membership, then select the minimum redundancy required.
94. Click *OK*.

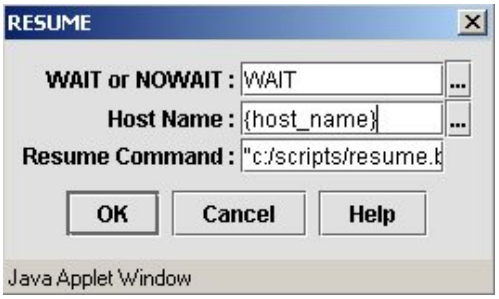
95. Double-click the *NORMALIZE* entry under Step/Sequence.



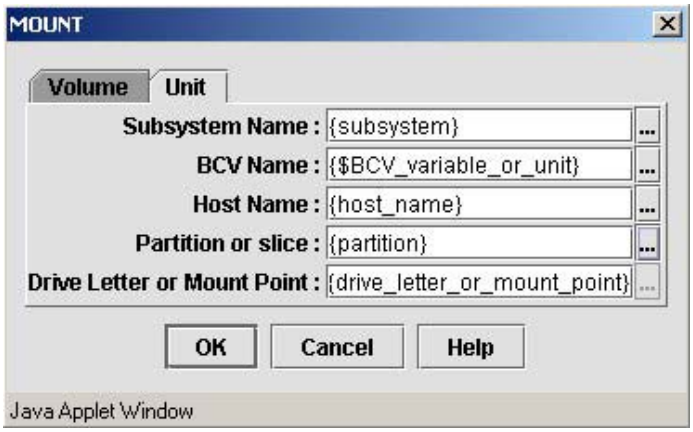
96. Select the *Unit* tab.
97. Click the ellipsis (…) beside Subsystem Name to display the available subsystems, then select an available subsystem.
98. Click the ellipsis (…) beside Unit Name to display the units available on that subsystem, then select an available unit.
99. Click *OK*.
100. Double-click the *SPLIT* entry under Step/Sequence.



101. Select the *Unit* tab.
102. Click the ellipsis (…) beside Subsystem Name to display the available subsystems and select an available subsystem.
103. Click the ellipsis (…) beside Unit Name to display the units available on that subsystem and select an available unit.
104. Click the ellipsis (…) beside BCV Name, and select *$BCV2*.
105. Click *OK*.

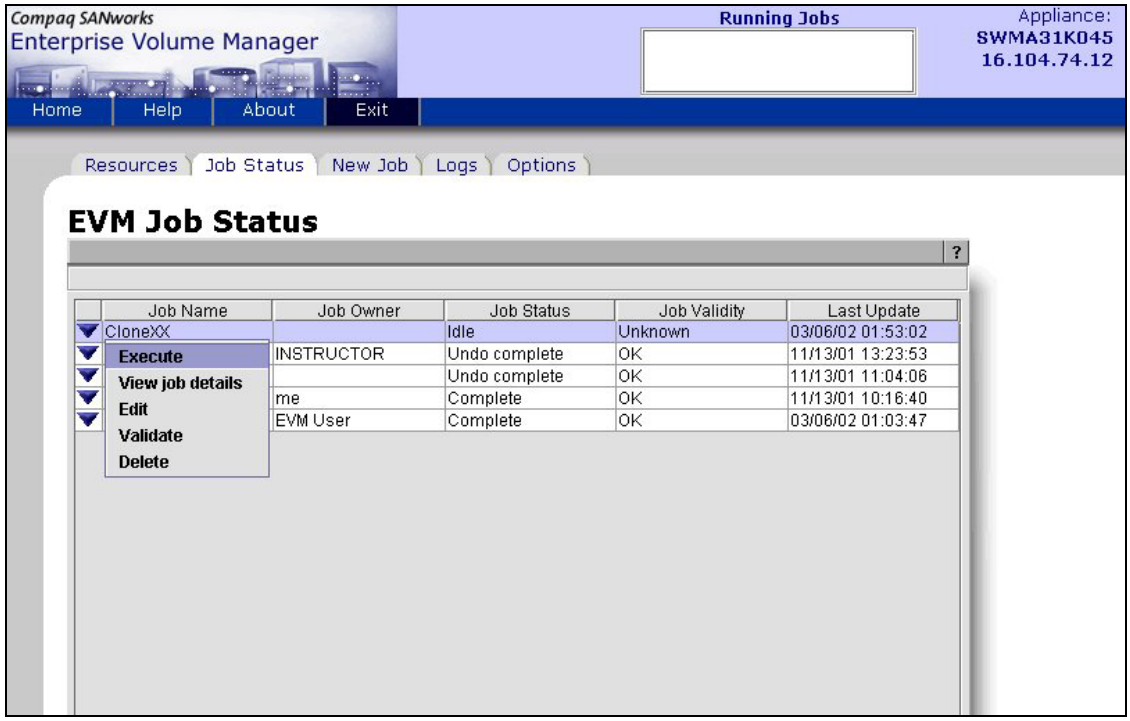


106. Double-click the *RESUME* entry under Step/Sequence.
107. Click the ellipsis (…) beside WAIT or NOWAIT to display the available options. Select *NOWAIT*.
108. Click the ellipsis (…) beside Host Name to display the available host, then select the host on which SQL Server is running.
109. Enter *"c:/scripts/resume.bat"* in the Resume Command field.



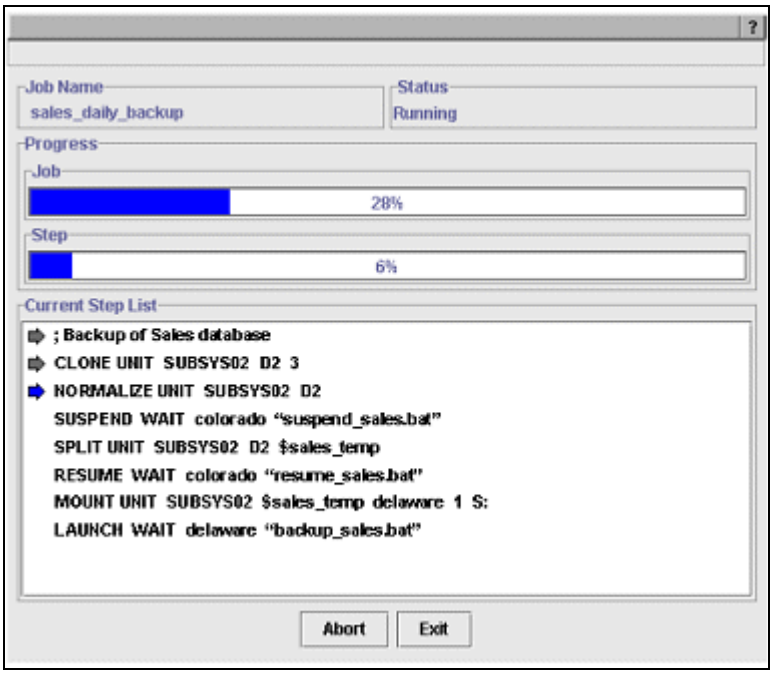
110. Double-click the *MOUNT* entry under Step/Sequence.
111. Select the *Unit* tab.
112. Click the ellipsis (…) beside Subsystem Name to display the available subsystems, then select the same subsystem as you selected in the SNAP parameters.
113. Enter *$BCV2* as the BCV Name.
114. Click the ellipsis (…) beside Host Name to display the available hosts, then select your data-mining application server.
115. Click the ellipsis (…) beside Partition or slice to display the options available, then select partition *1*.
116. Enter *Y:* as the Drive Letter or Mount Point.
117. Click *OK*.

118. Double-click last occurrence of the *LAUNCH* entry under Step/Sequence.
119. Click the ellipsis (…) beside Host Name to display the available hosts, then select the host on which the batch will be run.
120. In the Launch Command field, enter *"c:/scripts/ShowData.bat"*.
121. Click *Save* → *Exit* at the bottom of the New Job page.



122. Select the Job Status tab.
123. Right-click *CloneXX* (where *XX* is your class station number) and select *Validate*.

124. Right-click *CloneXX* (where *XX* is your class station number) and select *Execute*.



125. Right-click *CloneXX* (where *XX* is your class station number) and select *Monitor* to view the job in progress.

Note what you observe at each of the job steps.

First launch: .....

Second launch: .....

Suspend: .....

Clone: .....

Normalization: .....

Split: .....

Resume: .....

Mount: .....

Last launch: .....

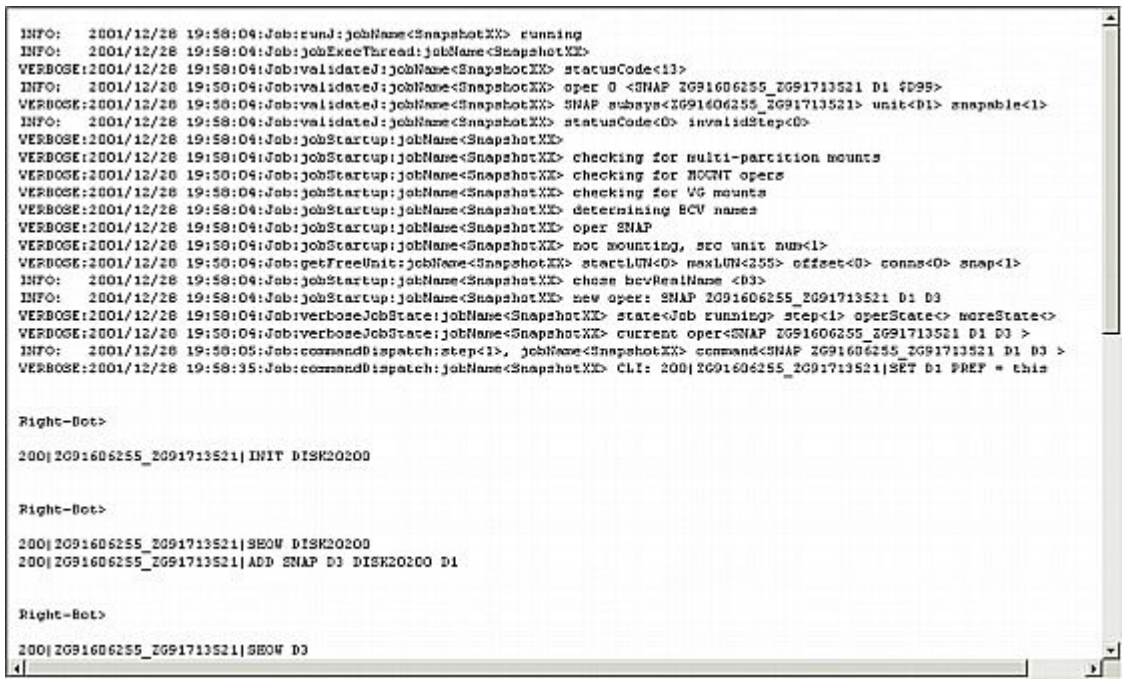
126. When the job is complete, click the *Job Status* tab to return to the list of available jobs.

What is the status of CloneXX?

.....

What options are available when you right-click *CloneXX* (where *XX* is your class station number)?

.....



127. Select the *Logs* tab, then double-click the first text file for your job (for example, job_CloneXX_1.txt) and view the list of commands that were executed when the job was run.
128. On your data-mining application server, right-click *My Computer* and select *Manage*.
129. Right-click *Storage* → *Disk Management* and select *Rescan*.
130. Verify that disk Y: is mounted on that server.

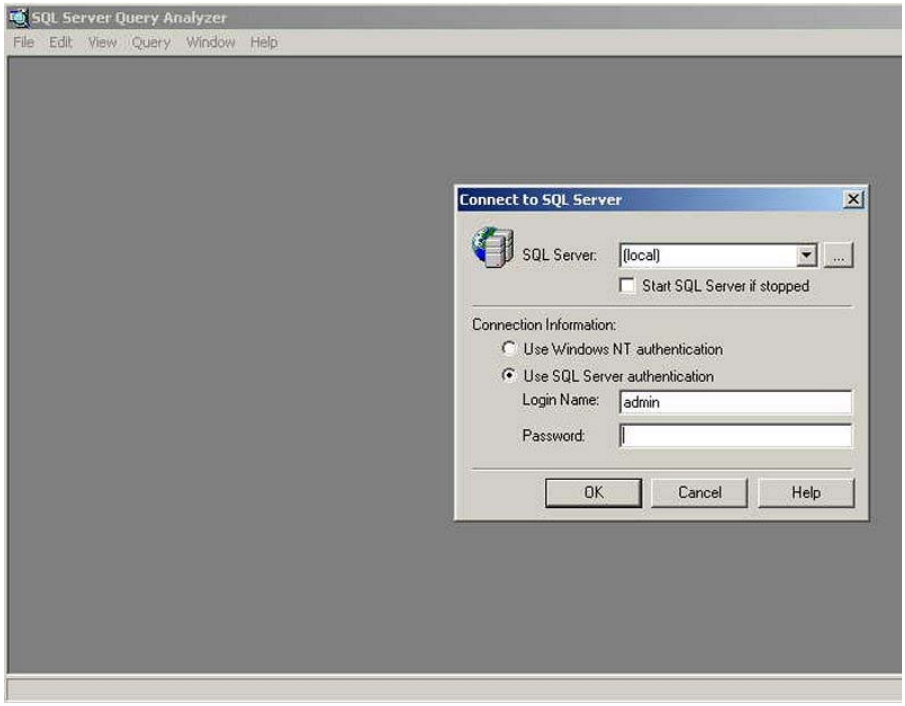
Exercise 3 — Snapshot Data Recovery

In this exercise, you will start a simulated application and corrupt (delete) the data.

Note

Your instructor will point you to the files necessary to start the application data simulation.

1. Using Windows Explorer, find the executable *c:\MSSQL7\BINN\iSQLw.exe*. Double-click *iSQLw.exe* to execute the file.



131. Log in admin with the admin user ID and no password. Use the defaults for any other parameters.
132. Select *File* → *Open* → *c:\scripts\ShowData.sql*.
133. The SQL statement in this query displays the data created in the database during the EVM jobs.
134. Click the green arrow (run) icon in the menu bar to execute the SQL script.
135. Verify that the Results tab shows data in the database.
136. Close *iSQLw.exe*.
137. Using Windows Explorer, find the file *z:\data\PseudoApplicationDB_data.mdf.*

     What is the size of the data file? .....
138. Using Windows Explorer, find *x:\data\PseudoApplicationDB_data.mdf* on your snapshot disk (X:).
139. What is the size of the data file?

     .....

140. Using Windows Explorer, find *y:\data\PseudoApplicationDB_data.mdf* on your clone disk (Y:).

     What is the size of the data file? .....

141. Open the SQL Server management window from the system tray and click *Stop*.
142. Using Windows Explorer, delete the database log file *z:\data\PseudoApplicationDB_data.mdf*.
143. Return to the SQL Server management window and click *Start/Continue*.
144. Open *iSQLw.exe* again and rerun the query (steps 5 and 6).

     What was the result?

     .....
145. Return to the SQL Server management window and click *Stop*.
146. Restore both database files from the snapshot drive (X: [copy and paste]).

147. Return to the SQL Server management window and click *Start/Continue*.
148. Return to the WinSQL window. Select *File* → *Open* → *c:\scripts\ShowData.sql* and accept the default login parameters. Run the query (click green arrow icon).

    What is the result?

    .....

Exercise 4 — Managing Hardware Failure

In this exercise, you will simulate hardware failure and data recovery.

1. Determine which disks were used in the original logical drive (drive Z:) and remove those disks from your subsystem.

149. Return to the iSQLw.exe window and rerun the query *ShowData.sql*.

150. What is the result?

.....

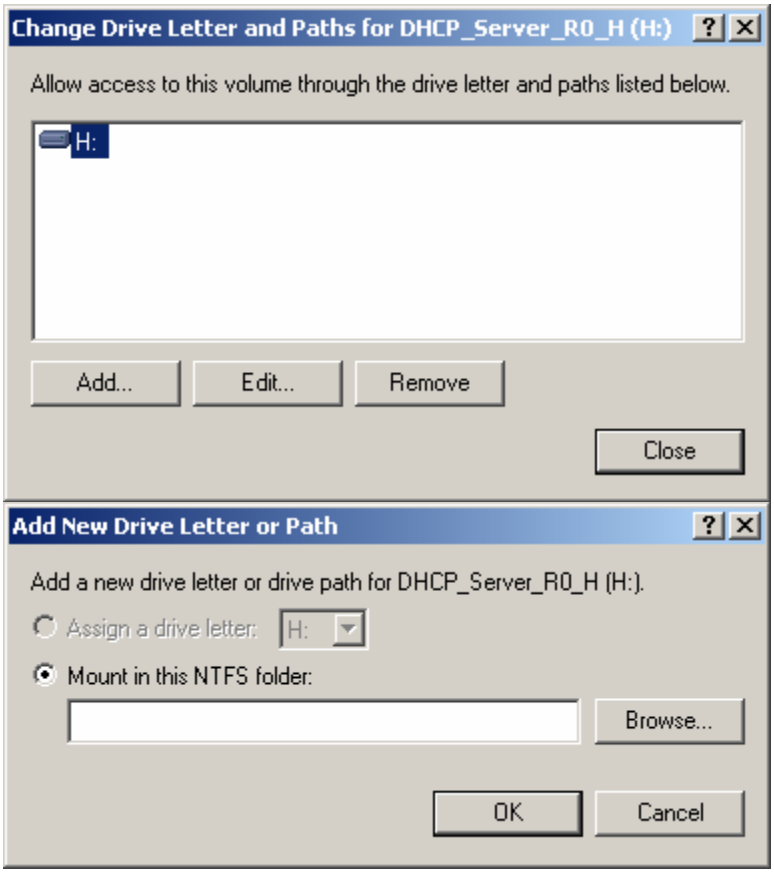
151. Close iSQLw.exe.

152. Return to the SQL Server management window and click *Stop*.

153. Attempt to recover the *PseudoApplicationDB_data.mdf* file from the snapshot drive (X:).

154. What is the result?

.....



155. Select *My Computer* → *Manage* → *Disk Management* → *Change Drive Letter and Path*, and change the drive letter to (Z:).

156. Return to the SQL Server management window and click *Start/Continue*.

157. Return to the iSQLw.exe window. Select *File* → *Open* → *c:\scripts\ShowData.sql* and accept the default login parameters. Run the query (click the green arrow icon).

    What is the result?

    .....

Exercise 5 — Restoring the Settings

1. Return the removed disks to the disk cabinet.
2. Return to the EVM Job Status page.
3. Right-click *SnapshotXX* (where *XX* is your class station number) and select *Undo* to release the resources used in the snapshot.
4. Right-click *CloneXX* (where *XX* is your class station number) and select *Undo* to release the resources used in the clone.

   When steps 2 and 3 are complete:

   a. Restart your computer.

This completes these exercises

Let your instructor know that you are finished

Objectives

After completing this lab, you should be able to:

- Understand the installation and operation of Secure Path software.

Prerequisites

- 1 HSG80-based storage subsystem
- 2 HSG80 controllers configured as follows:
  - Dual redundancy (transparent failover mode)
- At least four disk drives installed in the drive cabinet
- At least one LUN (D1) created beforehand.
- 1 host running Windows 2000 (SP2 or later) with two 64-bit 33MHz Fibre Channel host bus adapters (HBAs)—1 HBA installed initially
- One browser station running Windows 2000 with Internet Explorer 5.5 or greater
- One Management Appliance
- 6 fiber cables
- Two Fibre Channel switches (8- or 16-port models)
- Your instructor will provide you with the following:
  - Location of Secure Path and Secure Path Manager software. Write this location in the space provided below:

    .....
  - Client and server can communicate via TCP/IP on the classroom LAN. Record the IP addresses of your client and server in the space provided below:

    .....

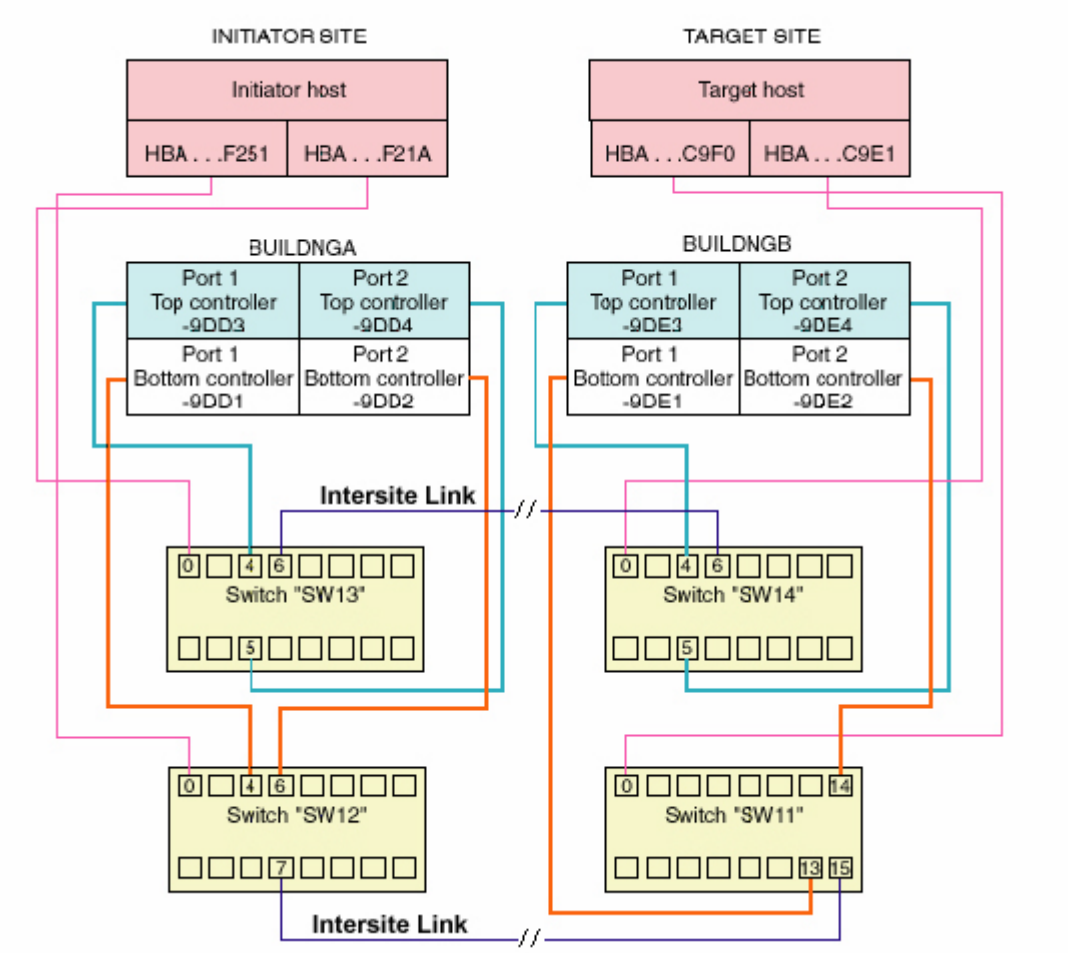
Checklist

Upon completion of each lab exercise, have your instructor verify that you have performed it successfully. Then check off the following list:

- ☐ Able to successfully install Secure Path as demonstrated by the successful failover of a degraded path.
- ☐ Able to manage a Secure Path profile by installing Secure Path Manager on the Management Appliance, configuring the client list and access rights, and running the Secure Path Manager interface.

Hardware Configuration and Physical Connections

When the lab station installation is complete, your station and your partner station should be configured as shown in the diagram below:



Cabling Secure Path for DRM

Verify the following:

- All fiber cables are properly seated.
- The ACS version of the controller is appropriate for the topology you are using. For example, if you are using ACS8.7P, you will not be able to conduct this lab within an arbitrated loop topology.

> **Note**
> This lab can be run in a FC-SW or FC-AL environment. However, this lab assumes that you will be working with a FC-SW. If necessary, a hub can easily be substituted for a switch. If you have any questions regarding the use of a hub, please ask your instructor for assistance.

- A maintenance (serial) cable connects your client station (or server) to the top HSG80 array controller. You can communicate to the subsystem using command line interface (CLI) or StorageWorks Command Console (SWCC).
- One HBA device and class drivers are loaded and they are functioning properly.
- On the server system, launch Event Viewer and ensure that hszdisk.sys has been started successfully (you must have at least one LUN configured on your controllers; additionally, that LUN must be formatted with an assigned drive letter).

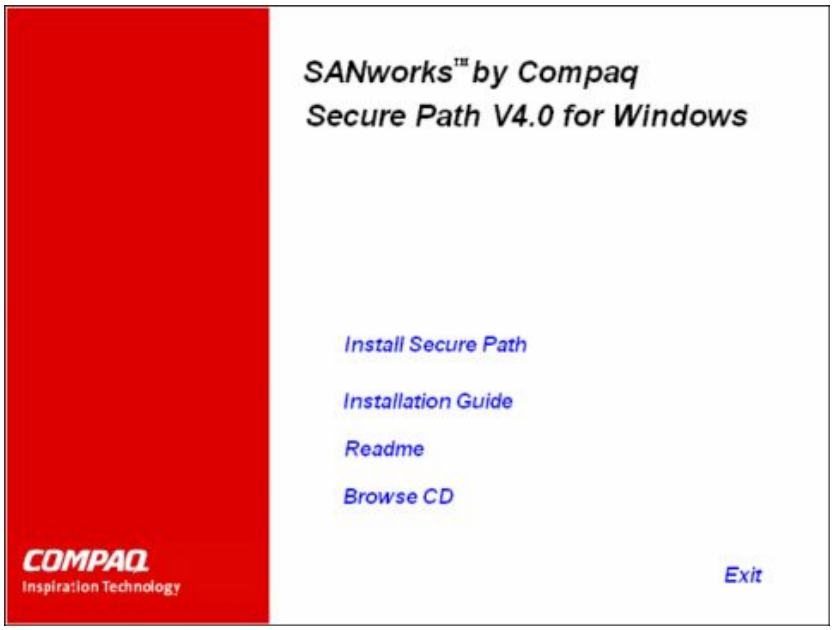
> **Note**
> To match this lab exercise, make sure you have at least two LUNs configured in your subsystem. This lab assumes one is labeled "Y" and the other "Z".

- In Event Viewer, make sure there are no errors related to your Emulex adapter.
- Ensure that:
  - Your controllers are in dual-redundant transparent failover mode and working properly.
  - You do not have any partitioned LUNs created behind your controllers (Secure Path v4.0 does **not** supported partitioning of LUNs).
  - None of your Windows 2000 volume sets use software RAID or extended volumes (for instance, you cannot span more than one physical disk).
  - The server has the TCP/IP protocol installed (the Secure Path manager and agent communicate through sockets).

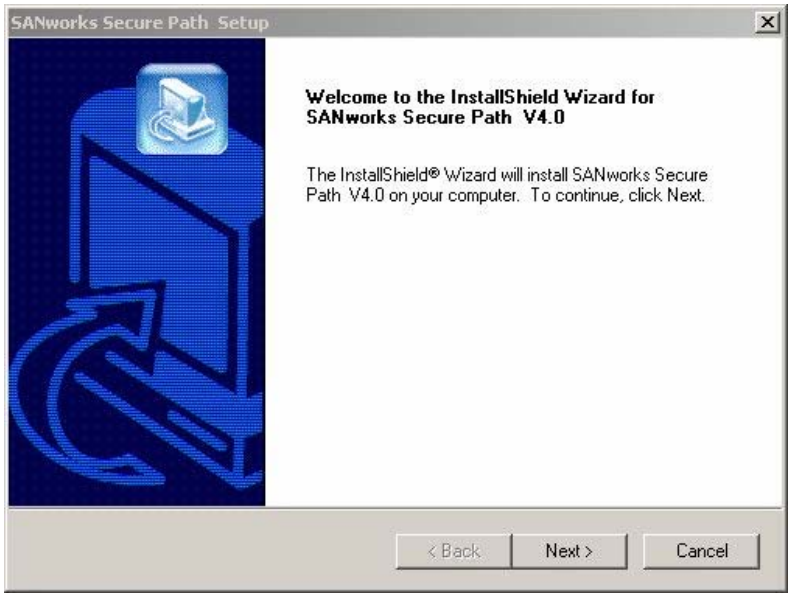
Installing the Secure Path Driver

Secure Path for Windows 2000 consists of a kernel mode filter driver (RaiDisk.sys) that is responsible for directing I/O to the desired path, and for changing paths whenever the driver detects a failure in a redundant path.

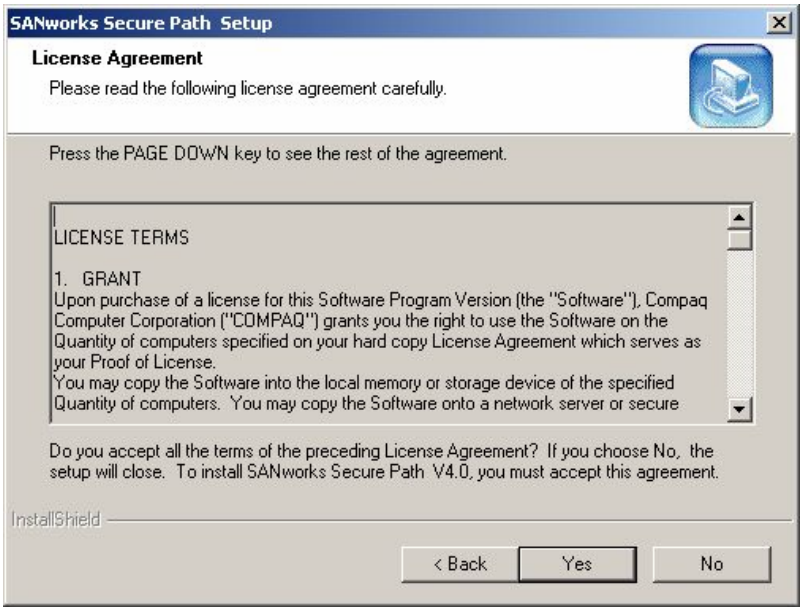
1. Locate the Secure Path installation files as directed by your instructor. Double-click *automenu.exe*.



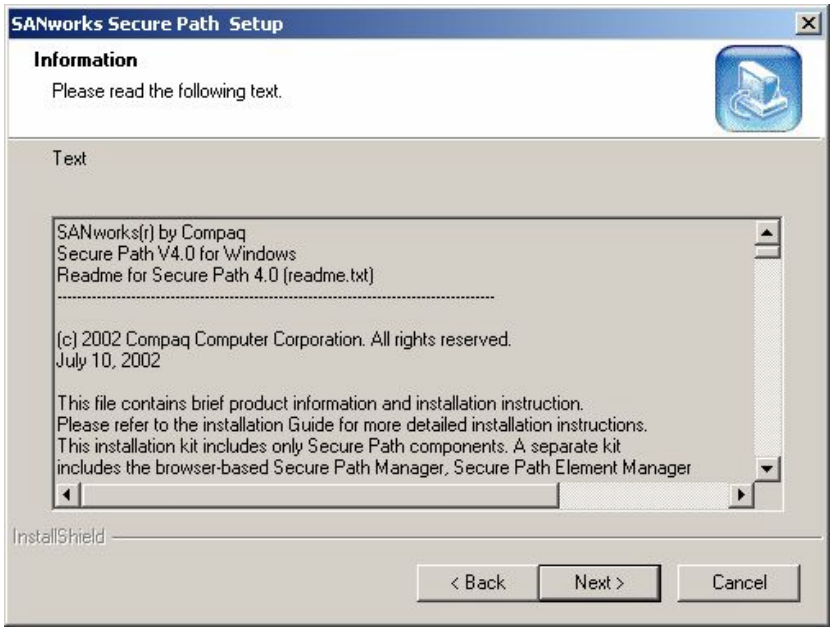
2. Select *Install Secure Path*.



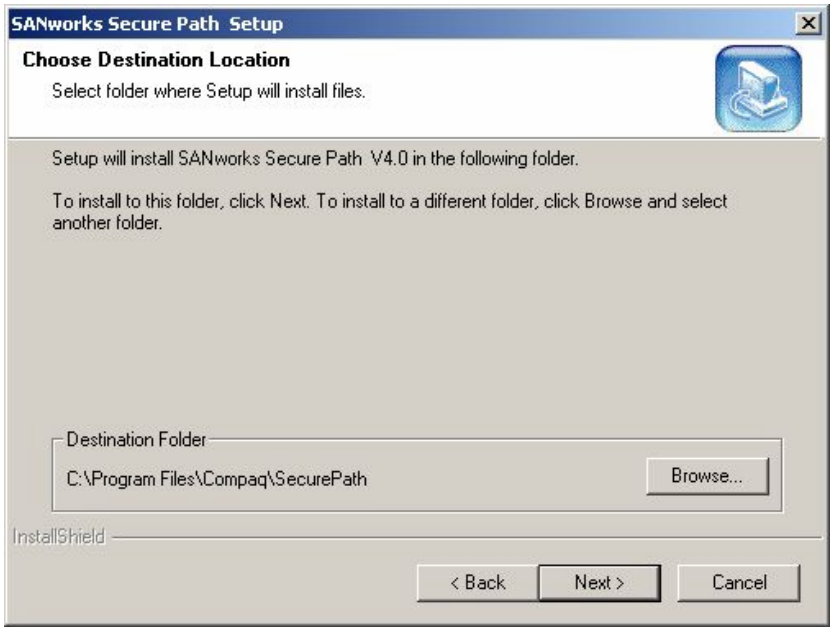
3. The Secure Path splash screen displays. Click *Next*.



4. The next screen Secure Path license agreement displays. Click *Yes* to agree to the terms and proceed with the installation.



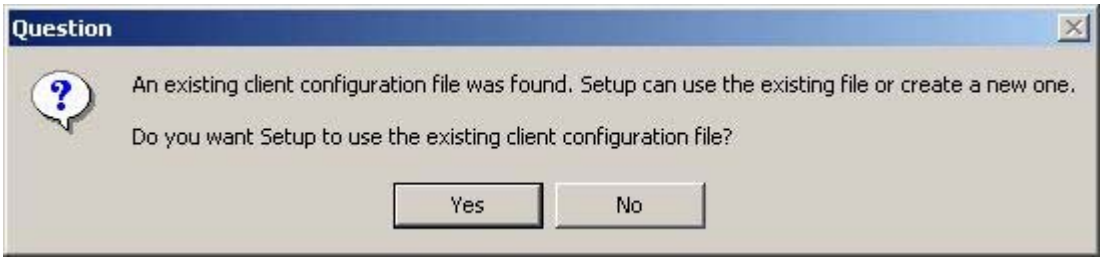
5. The next dialog box displays Secure Path release information. Scroll down the list to examine this text. When you have finished, click *Next*.



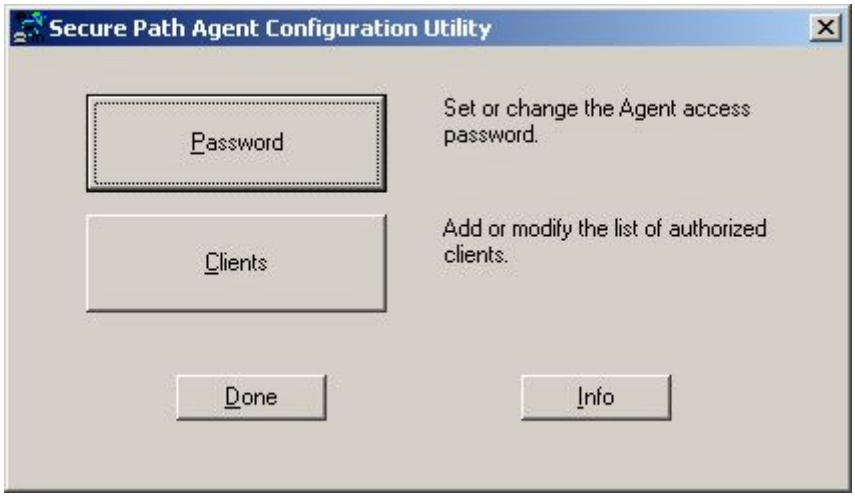
6. The next screen prompts you for the Secure Path installation directory. Accept the default and click *Next*.

Important

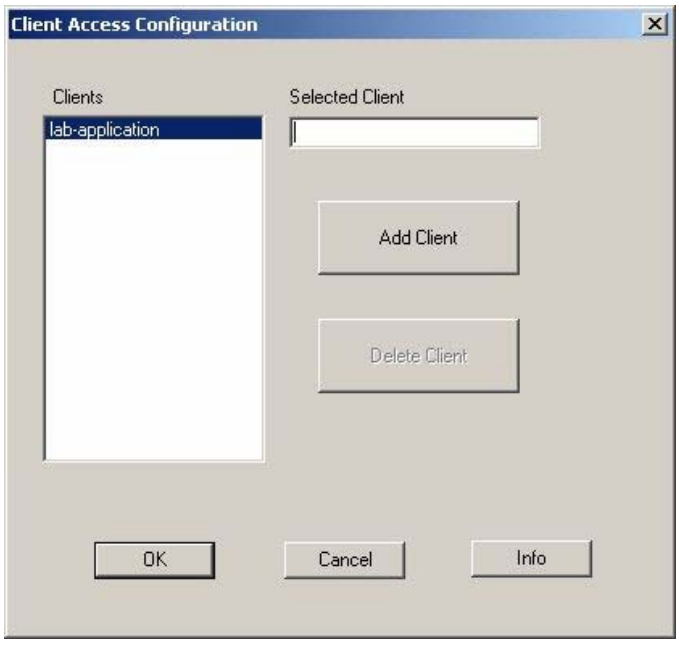
Select *No* if prompted to overwrite your current HSZdisk or HBA drivers with older versions.



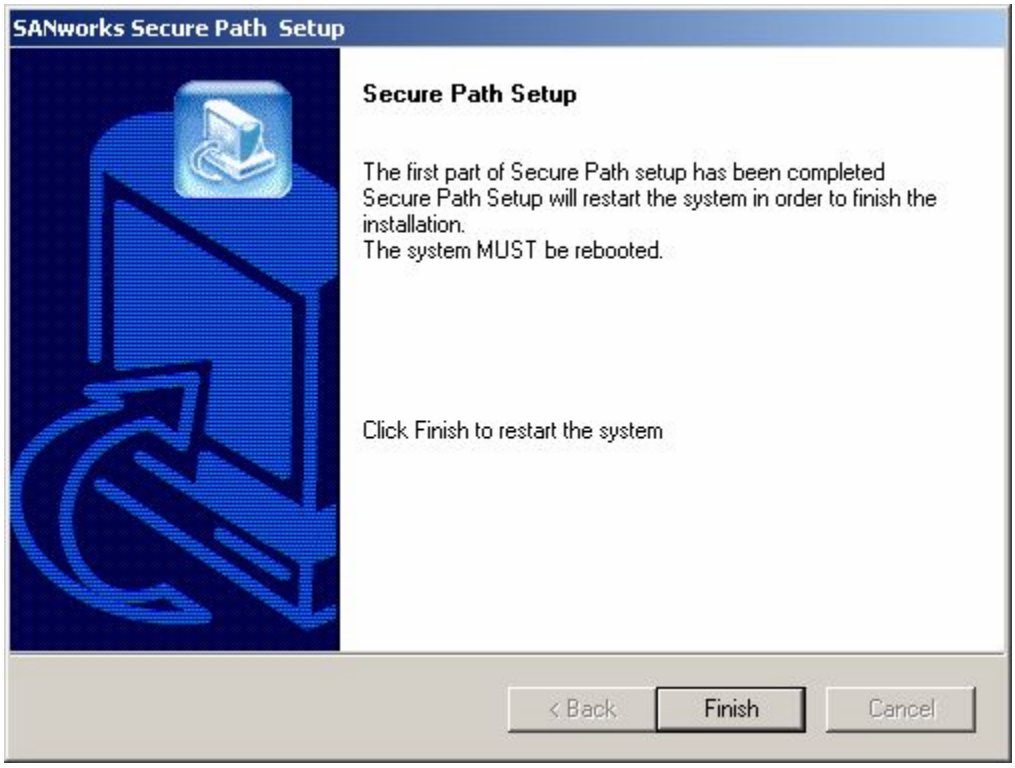
7. If setup notifies you that you have an existing configuration file, click *No* to the question of using the existing file.



8. The Secure Path Agent Configuration Utility selection displays.
   a. Click on the *Password*. Enter and confirm *12345* as your password. You will be asked for this password when you create Secure Path Manager profiles later in this lab.
   b. Click *Clients* to configure the list of clients that will be able to manage this instance of Secure Path.
   c. The Clients dialog box displays:



   d. Enter your computer name as the client.
   e. Click *Add Client*.
   f. Click *OK*. You will return to the dialog box with the *Password* and *Clients* buttons. Click *Done* to continue.



9. Click *Finish* to end the installation and allow the system to reboot.

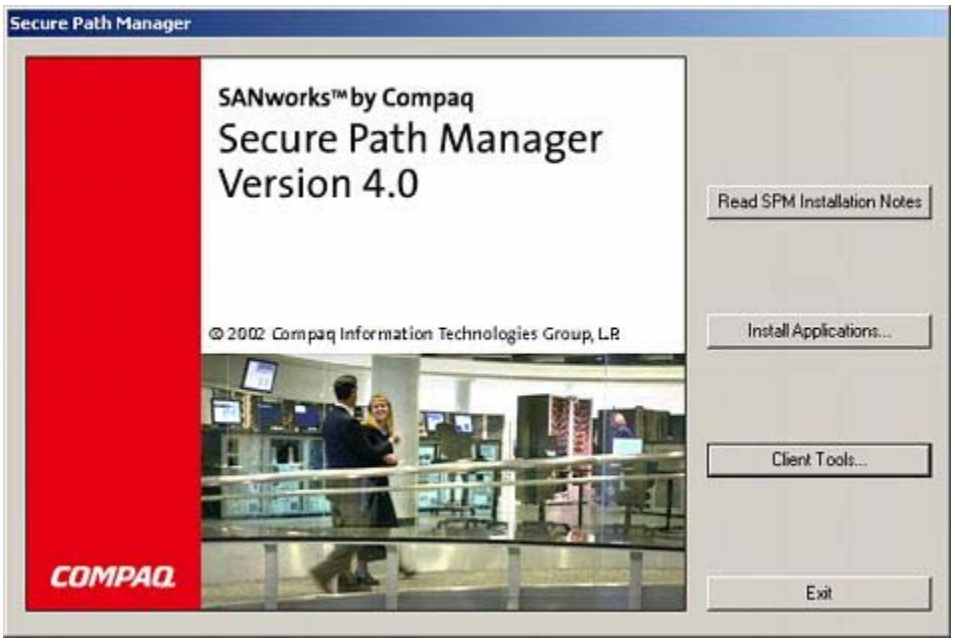
Installing Secure Path Manager

Secure Path is managed by a Secure Path Manager, which can be installed on a management server or the Management Appliance. Secure Path Manager can be installed on the same server as the Secure Path agent and can be run remotely through a web browser. For this lab, we will install Secure Path Manager on the same server as the Secure Path agent.

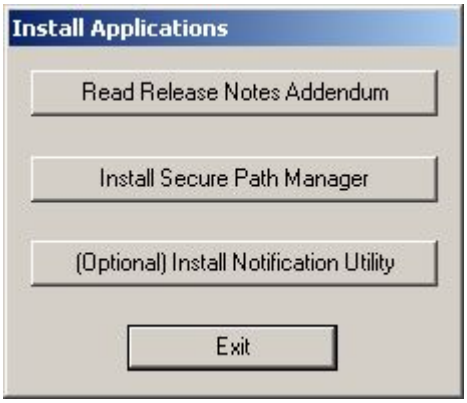
Note

To install Secure Path on the Management Appliance, insert the Secure Path CD into the CDROM of the Appliance. Use Open SAN Manager CD installation to complete the install.

1. Locate the Secure Path installation files as directed by your instructor. Double-click *automenu.exe*.

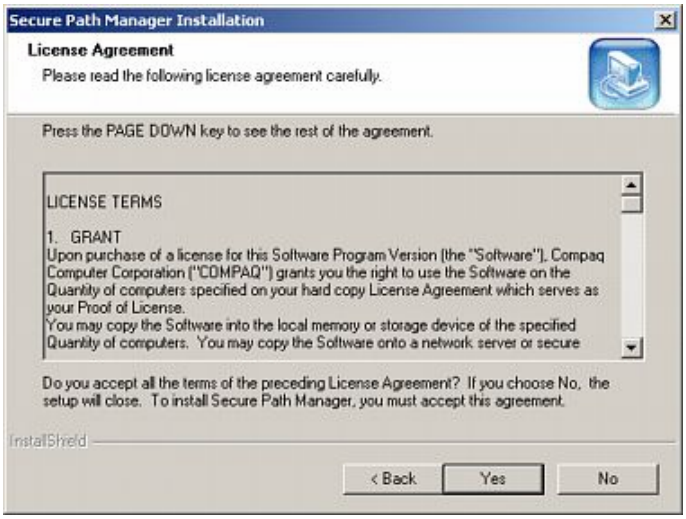


2. Select *Install Applications*.

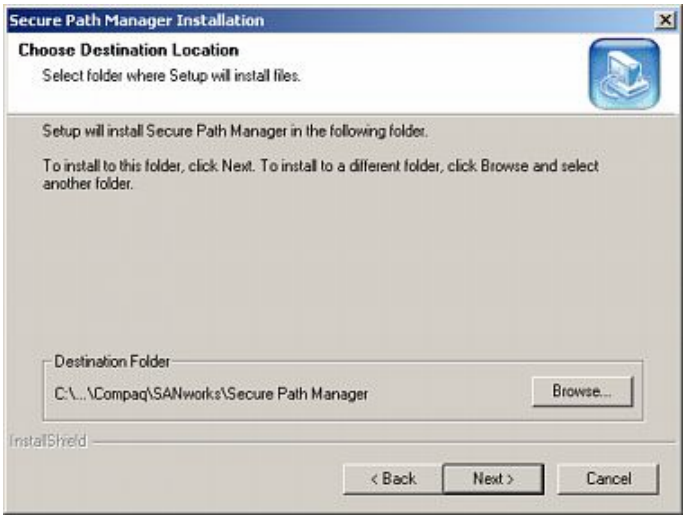


3. Select *Install Secure Path Manager*.

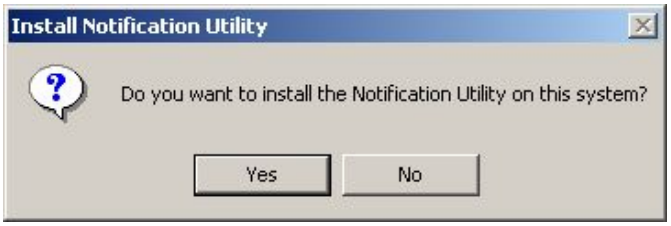
4. Click *Next*.



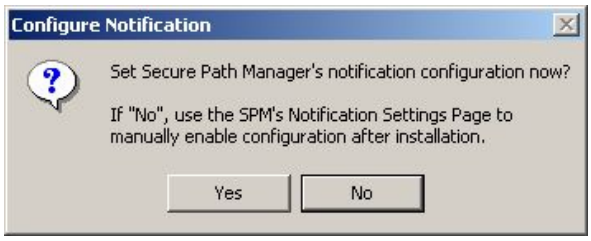
5. Click *Yes* at the license agreement.



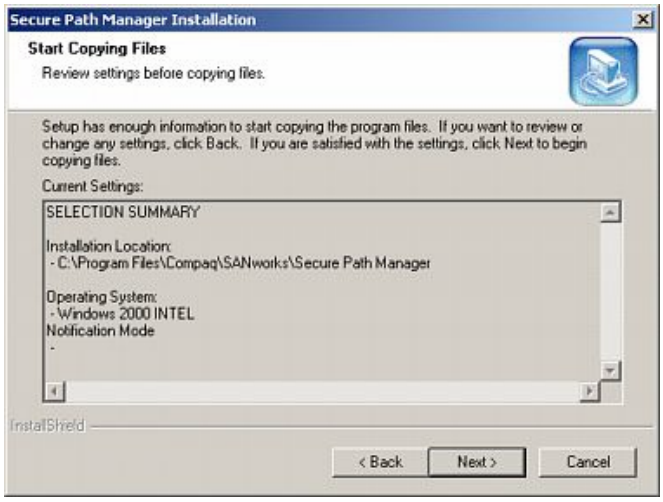
6. Accept the default installation destination, click *Next*.



7. Click *No* to install the Notification Utility on this system.



8. Click *No* to Configure Notification.



9. Review the setting and click *Next* to begin the installation.

10. Click *Finish* to complete the installation of Secure Path Manager

Setting Your HSG80-based Storage System to Multiple-Bus Failover Mode

> **Important**
> The controller is configured **after** installing Secure Path on the host. This is the sequence that **must** be followed when installing Secure Path software.

Initiate a CLI session from your server system to your HSG80.

Enter:

```
SET NOFAILOVER
```

Take the controllers out of transparent failover mode. The other controller will shut down. Restart it by depressing its OCP Reset button, and wait a couple minutes for it to come back up

```
SET MULTIBUS COPY = THIS
```

Set the controllers in multiple-bus failover mode. Note that both controllers will be restarted in the process

```
SHO THIS
```

Verify that this controller is in multiple-bus failover mode.

```
SHO OTHER
```

Verify that the other controller is in multiple-bus failover mode.

Preferring Units Between Your Controllers

You should prefer (assign) storage units to one of the two controllers to specify which controller will be used to access the unit during server boot. That is, you determine which controller will be doing the work for which units. In effect, this procedure specifies which path (controller, fabric, and HBA) the I/Os will travel.

You have the option of moving units around the two paths from within the Secure Path Manager. For now, take the recommended action of splitting storage containers evenly between the two paths.

Enter:

```
SHOW UNITS
SET D1 PREF = THIS
SET D4 PREF = OTHER
```

> **Note**
> Notice that units are initially set to `NO_PREFERRED_PATH`. This lets the operating system dictate which path to choose. In general, because unpredictable load balancing would occur, you would **never** want to do this.

Installing the Second HBA

1. Shut down your Windows server. Install another HBA and Fibre Channel SAN Switch as the diagram below shows:

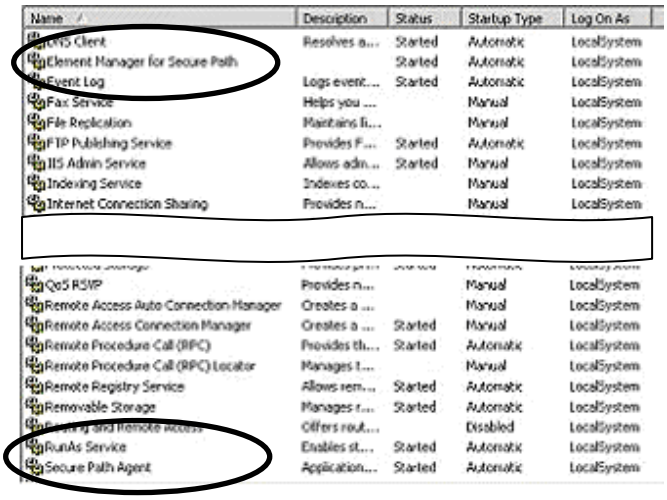
Note
Use the ports and configuration as shown in the graphic on page 2 of this lab.

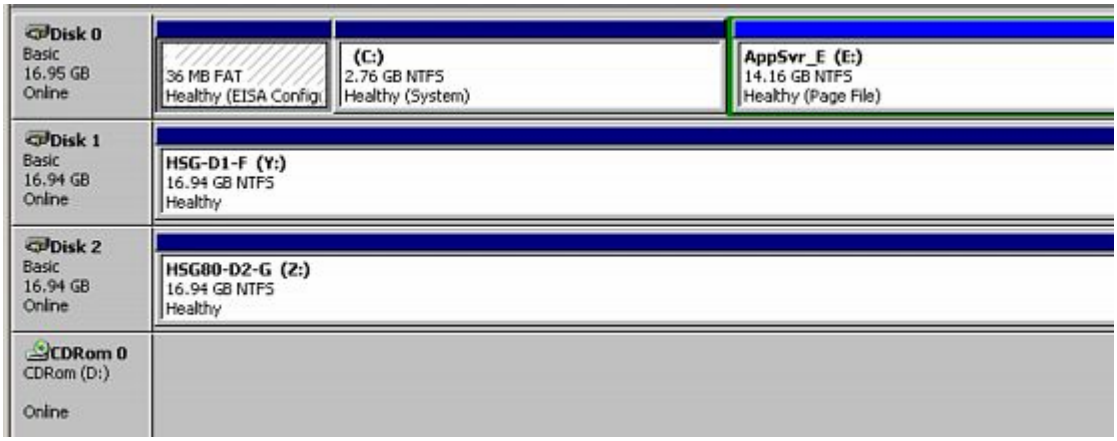
2. Power on the server.

Important
Remember to press *F10* and run the System Configuration utility so the new HBA will function correctly.

Verifying the Secure Path Hardware Configuration

After the server restarts, verify that the Secure Path Agent and Secure Path Element Manager have started (right-click *My Computer* → *Manage* → *Services and Applications* → *Services*).

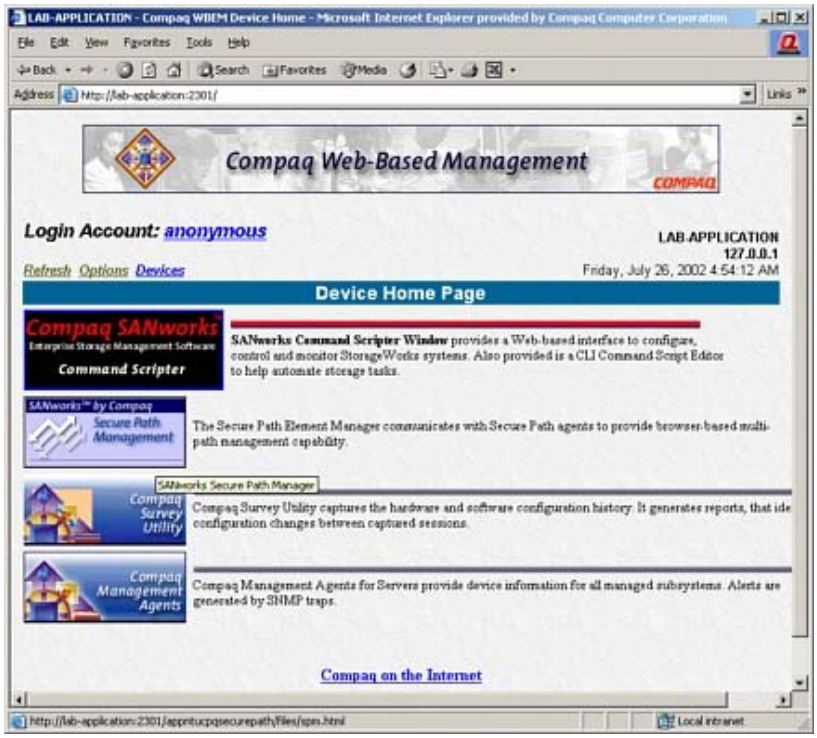




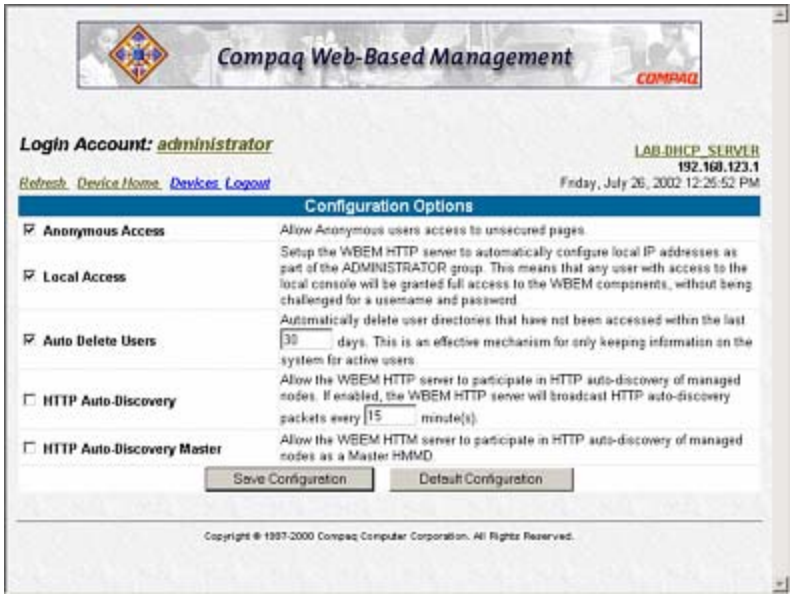
Verify that each unit configured behind the controllers only has one disk number listing under Disk Administrator. If the installation had gone awry, you would see two instances of each unit shown above.

The Secure Path Manager

Logging in to the Secure Path Manager



1. Open a browser window and browser to the localhost for the Secure Path management station and log in.

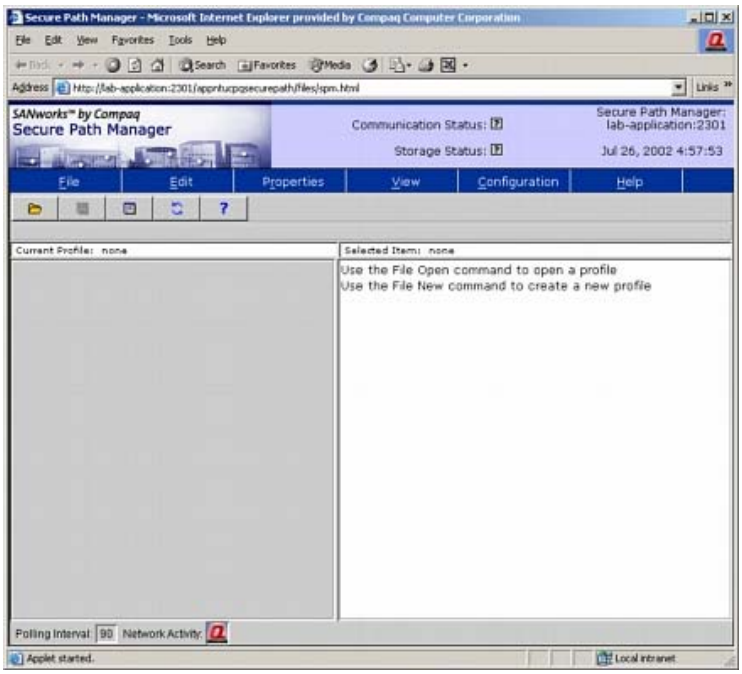


2. Log in, select *Options* and ensure that local and anonymous access is enabled.

Note

If Java is not installed, you will be required to install it before continuing with this step.

3. Select *Secure Path Management*.



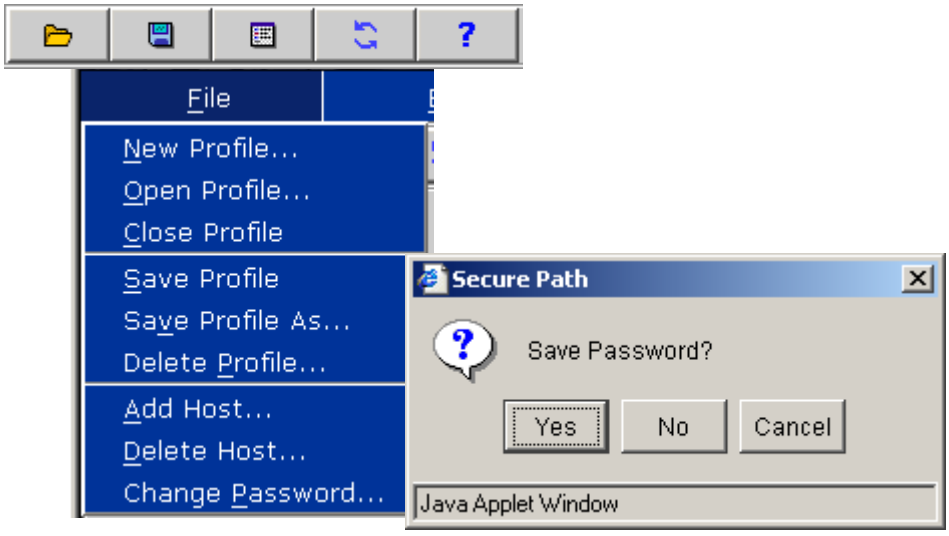
Since this is the first time the Secure Path Manager is being run, you will have to create a profile to use when accessing the Secure Path agent.

4. Select *File* → *New Profile*.

3. Enter the profile name as shown above substitute your station number for *XX*.

4. Enter *12345* as the password (Note: This is the same password used earlier in the installation).

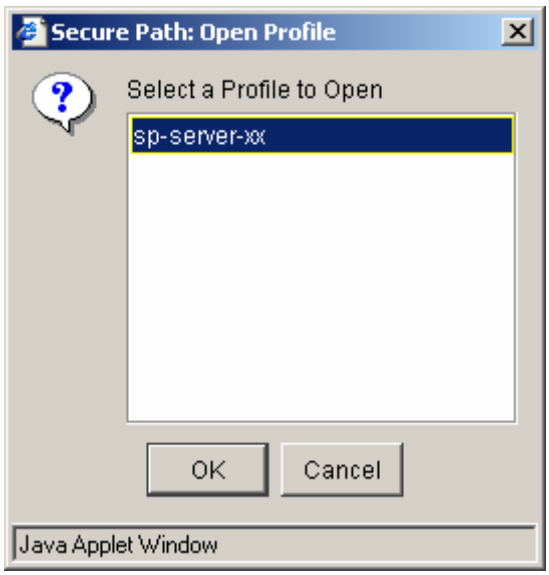
5. Enter your Secure Path Management Server name for the host name.
6. Click *Add* → *Done*.



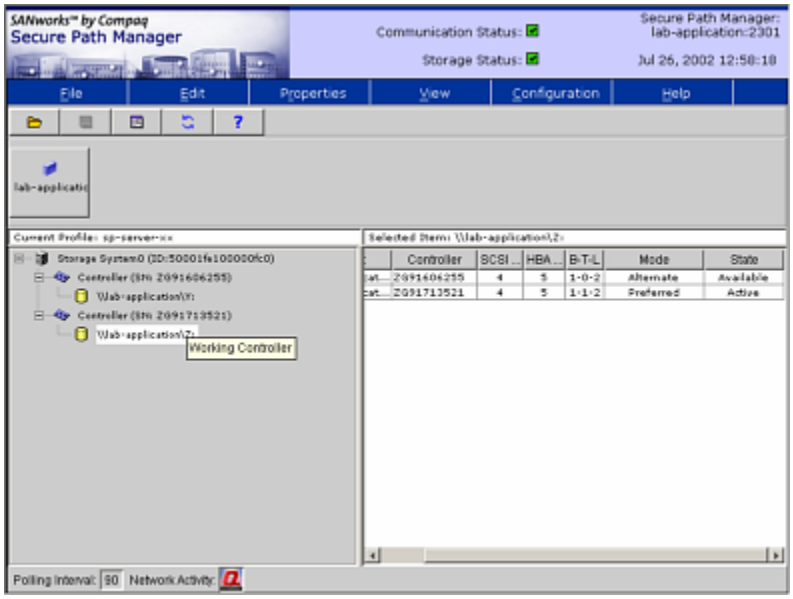
7. Click the disk icon (or *File* → *Save Profile*) → *Yes* to save the profile.

Important

The password and client list for the Secure Path agent can be modified by selecting *Start* → *Programs* → *Secure Path* → *SecurePathCfg*.



8. Click folder icon (or *File* → *Open Profile*) and open the profile you just created.



9. Expand the storage system and controllers and view the associated path information.

   The Secure Path manager shows both paths to your storage subsystem. The top path shows Controller A and the bottom path shows Controller B.

   Information regarding each disk device is displayed in the right hand pane.

10. Using your mouse, click-and-hold on disk Z and drag it to the other controller.

Note

Dragging disk devices between the two paths is the method used to load balance each controller path. Remember to change the associated PREFERRED_PATH on the HSG80 controller when you do this (for instance, SET D1 PREF = OTHER). Otherwise, the next time the Windows server is restarted, the original PREFERRED_PATH unit setting will take precedence and place your disk back in its original path.

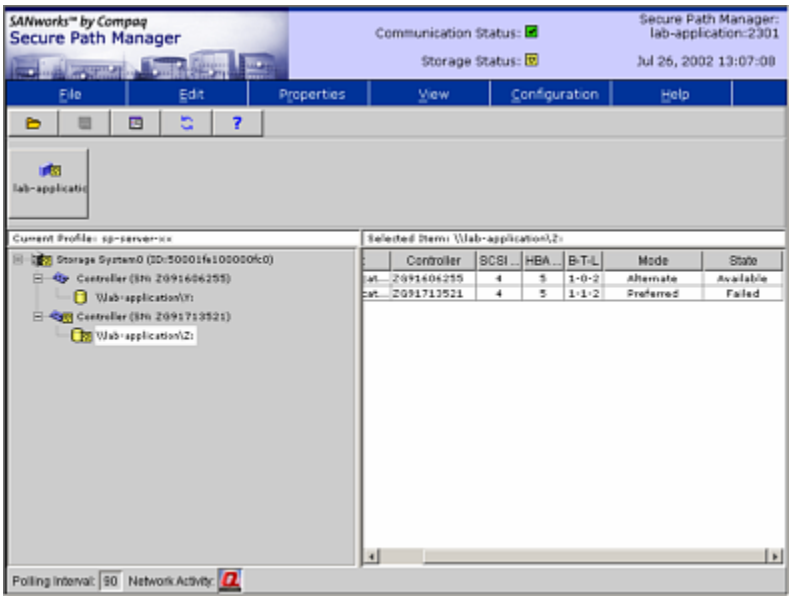
Testing the Secure Path Software

You will now test the functionality of the raidisk.sys filter driver.

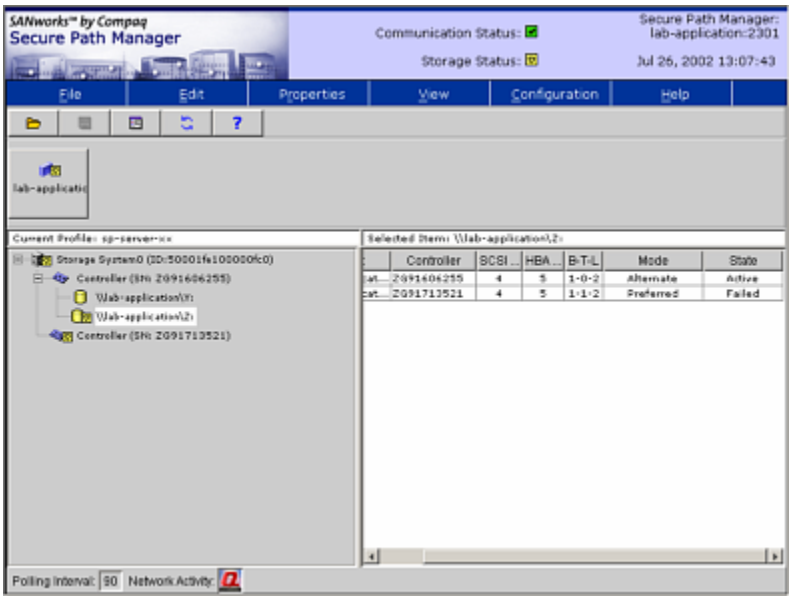
1. Note which controller is controlling *Disk Z*. This gives you the controller serial number of the controller for *Disk Z*. Using your CLI interface, determine which controller corresponds to that controller serial number. Note which controller is being used as well as the switch (or hub) and HBA that are used to access the subsystem.

2. Start a copy of your system drive (probably drive *C:*) to drive *Z:*. After the copy begins, pull out the power plug going into the switch (or hub) used with drive Z.

   The following graphic show the result of the error that the Secure Path GUI will display:



The following graphic shows the result of the path failover.



Note

Notice that the copy continued without error and that disk Z icon changed to indicate that it is *Using an Alternate Path.*

3. If Auto Failback is enabled for that host, continue to refresh the screen and note that the path fails back to the original controller. (Hint: View the polling interval to determine how long it will take before the failback occurs).

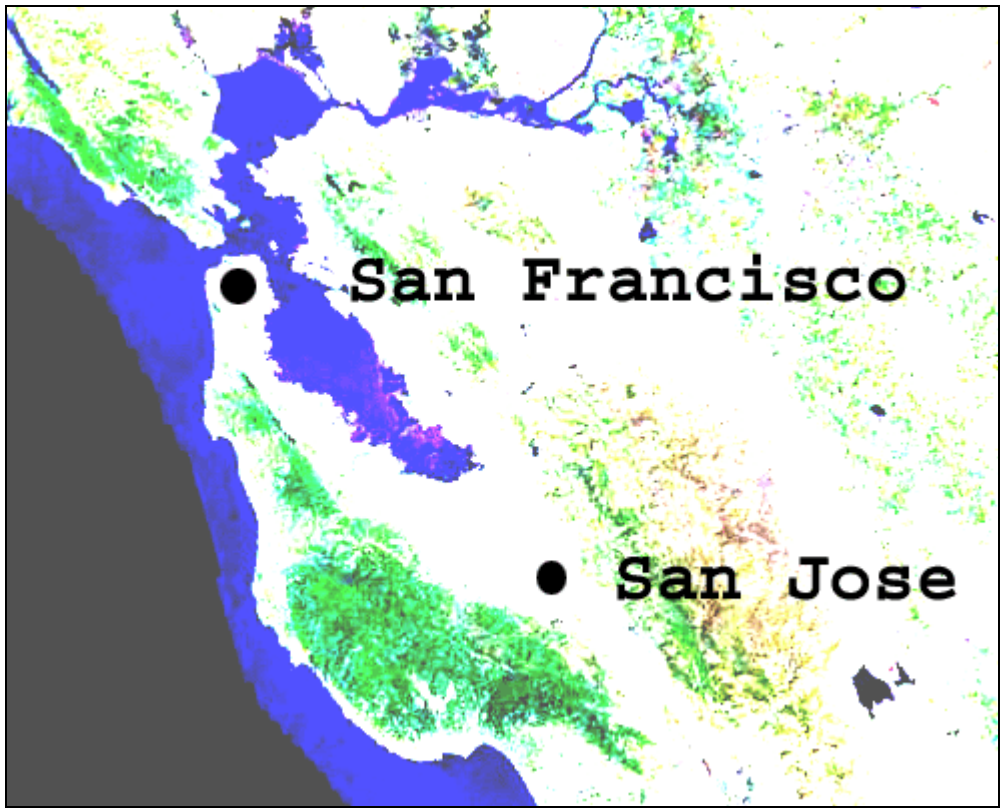
This completes this lab exercise

Please notify your instructor that you are finished

hp StorageWorks data replication manager installation

lab 4

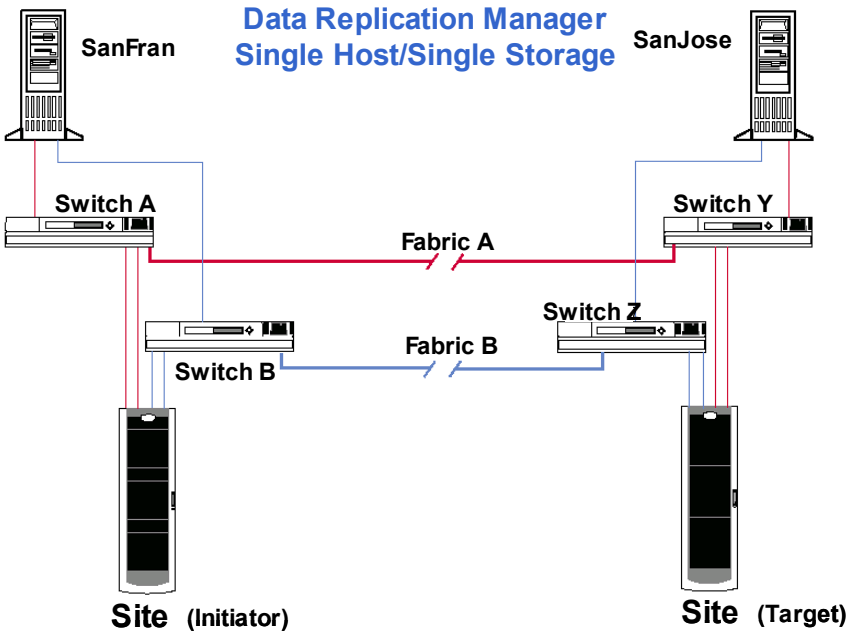
Objective



Your customer, Widget Inc., is concerned about disaster tolerance and the availability of the company's data. Widget Inc. is based in San Francisco, CA. Widget also has a field office in San Jose, CA. There is concern about power outages that occur frequently in the San Francisco area. The company has invested in a backup generator and UPS equipment, but is still concerned that their data may become unavailable. Their concern is warranted; the loss of connectivity to their database can cause the loss of millions of dollars in a very short time.

The following lab exercises will allow you to configure an HP StorageWorks Data Replication Manager (DRM) solution for the Widget company. The IT staff of Widget would also like to see a demonstration of the failover process. They would like you to perform an unplanned failover to San Jose using a sample database.

Solution



Conn Name	WW Name	Host Name	HBA Number

Note

For the syntax of any CLI commands included in this lab, see the *HSG80 Array Controller ACS Version 8.6 CLI Reference Guide*.

Prerequisites — Both Sites

! Important

- For ease of cable troubleshooting, ensure that the Port cabling is identical for both SanFran (initiator) and SanJose (target) sites. For example, Port 1 from the top controller should be in the same Port on the switch for both SanFran and SanJose sites, and so on. Remember, under normal circumstances, SanJose is physically separate from SanFran.
- **Do not** cable the Inter-Switch-Link (ISL) until you are instructed to do so in the lab.
- **Do not** restart the host at SanJose (target) until you are ready to initiate a site failover.

1. Write down the World Wide Names (WWN) of all components at the SanFran and SanJose sites of the DRM installation. Use the table provided to record the names.
2. Cleanly uninstall HP storage software products **other than HP StorageWorks Secure Path**, which may have been installed earlier in the course.
3. Verify that the Secure Path lab was completed successfully, which requires that the controllers be configured for multibus failover.
4. Use Disk Administrator to delete any drives associated with the storage system that the host sees.
5. Verify that a terminal session is active on the upper HSG80 controller on both subsystems.
6. Microsoft SQL Server 7 Service Pack 3 or greater installed on both the initiator and target hosts (SanFran and SanJose)
7. Verify that all scripts associated with the simulated application are in the *c:\scripts* directory of the host computer.
8. Shut down the servers (hosts) at the SanFran and SanJose sites.
9. Run DILX on all units on both storage systems.
10. Delete any existing units, storagesets (containers), and connections on both storage systems.
11. Verify that controller Ports are set to fabric topology and that there are no controller errors.
12. Verify that SAN Switch 8, SAN Switch 16, SAN Switch 8EL or SAN Switch 16EL Fibre Channel switches are used.
13. Ensure that 12 hard drives (10000 to 60000 and 10100 to 60100) are configured for both storage systems (or any variation of disk numbers that equals 12 drives).
14. Verify that the controllers are in SCSI-3 mode.

.

Preparing the Switches

Switch Configuration

This lab is based on the use of StorageWorks SAN Switch 8 Fibre Channel switches. If you are using StorageWorks Fibre Channel Storage Switch 8 switches, set the following parameters through the front panel interface.

IP Address Assignment

Important

DRM requires that both switches at each site use the same Domain ID. For example, both switches at SanFran will use ID "1", and both switches at SanJose will use Domain ID "2".

Note

- During the configuration of the switches, press *Enter* after each command that is entered in the HyperTerminal window.
- Currently, HP only supports the Ethernet IP address for use in communicating with the switch. Check the storage website at **http://www.compaq.com/storage** for current information on supported protocols.

1. Begin with the SanFran (initiator).
2. Using HyperTerminal, establish a telnet connection to the switch. Ensure that the connection uses VT100 emulation.
3. When the connection to the switch is established, press *Enter* one time. The switch command prompt displays. If prompted for a username and password, the default username is "admin" and the password is "password."
4. To begin making configuration changes, disable the switch.

   Type `switchDisable`
5. Configure the switch.

   Type `configure`
6. Type `Yes` then press the *Enter* key to configure fabric parameters. Use Domain ID 1 for both switches at SanFran (initiator) and Domain ID 2 for both switches at SanJose (target).
7. Accept the default settings for the remaining parameters.

8. Verify the IP address that has been assigned to the switch.

   Type `ipAddrShow`

> **! Important**
> Check the current IP addresses. If they are configured as shown in the following table, skip the next step.

9. If necessary, change the IP address to match the classroom configuration.

   Type `ipAddrSet`

Unless instructed otherwise, use the following IP settings for all of the switches.

Location	Domain Name	Position	IP Address	Subnet Mask
SanFran	SanFran	Top	Server IP +1	255.255.0.0
SanFran	SanFran	Bottom	Server IP +2	255.255.0.0
SanJose	SanJose	Top	Server IP +1	255.255.0.0
SanJose	SanJose	Bottom	Server IP +2	255.255.0.0
Default Gateway	128.100.100.252			

10. Reenable the switch.

    Type `switchenable`

11. Type `exit` to leave the switch configuration utility.
12. Repeat this process for the remaining SanFran switch.
13. Repeat Steps 2 through 12 on SanJose (target) switches.

Configuring the Array Controllers

**********SANJOSE**********

On the Target Storage Subsystem (SANJOSE)

Note

- The container names at the target site and initiator site will be the same.
- Two drives in the initiator storage system (SanFran) will be saved for use by the logs.
- Preferred path assignments in this lab were arbitrarily selected. In a production environment, path preference would be assigned based on load balancing and expected disk activity planning.

1. Establish a CLI session with the storage subsystem using the same parameters you used to connect to the switch. If you have trouble connecting, verify that you are using the correct connection speed.
2. Identify all disk devices in the storage system.

   Type

   ```
   RUN CONFIG
   ```

3. Based on the customer configuration from the beginning of this lab, create, initialize, and assign LUNs to two containers as indicated in the following table.

Container	Disks	Units	Description
SQL_D_M	10000, 30000	D1	Application 1 data – mirrorset
SQL_L_M	10100, 30100	D2	Application 1 logs – mirrorset

   Type

   ```
   ADD MIRROR SQL_D_M DISK10000 DISK30000
   ADD MIRROR SQL_L_M DISK10100 DISK30100
   INIT SQL_D_M
   INIT SQL_L_M
   ADD UNIT D1 SQL_D_M
   ADD UNIT D2 SQL_L_M
   ```

! Important

If you name the units or mirrorsets with different names than what is listed in the preceding table, do not use dashes. Dashes are not supported with DRM scripting.

**********SANJOSE**********

4. Distribute the units by setting their preferred path.

   Type

   ```
   SET D1 PREFERRED_PATH=THIS_CONTROLLER
   SET D2 PREFERRED_PATH=OTHER_CONTROLLER
   ```

5. Disable access on all units.

   Type

   ```
   SET D1 DISABLE_ACCESS_PATH=ALL
   SET D2 DISABLE_ACCESS_PATH=ALL
   ```

   Important
   Disabling access to these units prevents the units from using connections that are already in place (although there should not be any if the prerequisites were followed).

6. Confirm that access has been disabled.

   Type

   ```
   SHOW UNIT FULL
   ```

**********SANFRAN**********

On the Initiator Storage Subsystem (SANFRAN)

1. Perform steps 1 through 6 from the previous “SanJose (target site)” section.
2. When you complete the above steps at both SanFran (initiator) and SanJose (target) sites, proceed to the next section of this lab.

**********SANJOSE**********

At SanJose (Target)

Important

- The name used in the REMOTE_COPY command is the name the controller pair you are configuring will present to the other set of controllers. It does not refer to the name used by the other controller pair.
- For OpenVMS environments, set device ID on all units with the following command: SET UNIT IDENTIFIER = value

Define the remote copy set name. This name will identify your controller to the partner site.

Note

Issuing this command will mask HBA access to Port 2 on both controllers. This command reserves Port 2 for DRM replication communication.

Type

```
SET THIS_CONTROLLER REMOTE_COPY=SANJOSE
```

Important

This command causes the controllers to restart.

**********SANFRAN**********

At SanFran (Initiator)

Define the remote copy set name at SanFran.

Type

```
SET THIS_CONTROLLER REMOTE_COPY=SANFRAN
```

Important
This command causes the array controllers to restart.

Configuring the DRM Controller

Connect the ISLs between the switches (Port 0 to Port 0).

**********SANFRAN**********

At SanFran (Initiator)

1. To create a remote copy set you must "bind" the units (LUNs) between SanFran and SanJose. In other words, pair a unit (D1) at SanFran with the same unit (D1) at SanJose.

> **! Important**
>
> - This command fails with the error ***Target connection name conflicts with a name already in the connection table*** but it creates and names the connections appropriately. In this exercise, the site names will be SANFRANA, SANFRANB, SANFRANC, and SANFRAND.
>
> This command does not have to be repeated for the remaining units at this time. Once the initial remote copy set has been created, the remaining connections are created automatically. These additional connections will be labeled based on the name of the initiator site and a letter.
> - A failure with the error ***Remote copy node SanJose not found or Fabric unavailable*** is an indication that there are cable or switch zoning problems.
> - A failure with ***Initiator unit specified not found*** indicates configuration problems.

Type

```
ADD REMOTE RCS_D1 D1 SANJOSE\D1
```

2. Ensure that the connections are created properly.

Type

```
SHOW CONN
```

3. Identify the WWN of each connection and its origination point.
4. Restart the host on SanFran.

The names for the remote copy sets and the unit name associated with each are defined in the following table.

Unit	Remote Copy Set Name	Description
D1	RCS_D1	SQL data – mirrorset
D2	RCS_D2	SQL logs – mirrorset

> **Note**
>
> The remote copy set name refers to the unit (LUN) at SanFran (initiator) as well as the unit it is paired with at SanJose (target). For example, RCS_D1 refers to unit (LUN) D1 at SanFran and unit (LUN) D1 at SanJose.

**********SANJOSE**********

At SanJose (Target) Site

1. Define a remote copy set at SanJose (target) site.

> **Important**
> - This command fails with the error ***Cannot find unit specified on Target controller***, but it creates and names the connections appropriately. In this exercise, the site names will be SANFRANA, SANFRANB, SANFRANC, and SANFRAND.
> This command does not have to be repeated for the remaining units at this time. Once the initial remote copy set has been created, the remaining connections are created automatically. These additional connections will be labeled based on the name of the initiator site and a letter.
> - A failure with the error ***Remote copy node SanJose not found or Fabric unavailable*** is an indication that there are cable or switch zoning problems.
> - A failure with ***Initiator unit specified not found*** indicates configuration problems.

Type

```
ADD REMOTE RCS_D1 D1 SANFRAN\D1
```

2. Show the connections.

Type

```
SHOW CONN
```

3. Identify the WWN of each connection and its origination point.

It is always a good practice to change the connection names to a more descriptive indication of where the connection to the storage system is coming from.

4. Rename the two connections that link Port 1 on the target controllers to the HBAs on SanFran to indicate their origination point.

> **Note**
> Because the host at SanJose is only active during a failover, this is the link to the HBAs on SanFran.

Type

```
RENAME !NEWCONNxx IT1
RENAME !NEWCONNyy IB1
```

If you do not see two connections, verify that your cables are correctly connected. Ensure that you see two connections before continuing.

> **Note**
> SanFran communicates with SanJose through host Port 2 on each controller (named SanFrana, SanJosea, SanFranb, SanJoseb, etc). Renaming the connections between host Port 1 at SanJose (target) and the HBAs to SanFran (initiator) is not required. However, it is a good practice use descriptive connection names for clarity.

**********SANJOSE**********

5. Enable the access paths to the connections you have just created.

   Type

   ```
   SET D1 ENABLE_ACCESS_PATH=SANFRANA,SANFRANB,SANFRANC,SANFRAND
   SET D2 ENABLE_ACCESS_PATH=SANFRANA,SANFRANB,SANFRANC,SANFRAND
   ```

6. Confirm that there is access to the SanFran connections.

   Type

   ```
   SHOW UNIT FULL
   ```

**********SANFRAN**********

At SanFran (Initiator)

1. Enable the access paths from the SanFran (initiator) site to the SanJose (target) site.

   Type

   ```
   SET D1 ENABLE_ACCESS_PATH=SANJOSEA,SANJOSEB,SANJOSEC,SANJOSED
   SET D2 ENABLE_ACCESS_PATH=SANJOSEA,SANJOSEB,SANJOSEC,SANJOSED
   ```

2. The following CLI command will create remote copy sets. When this command is entered, the controllers will copy all data from the SanFran (initiator) storage units to the SanJose (target) units. This process is called *normalization*.

   Note
   This is the same command that failed when entered originally. Because connections and access paths are now set, the command will not fail this time. This command "pairs up" the units that make up the Remote Copy Set. Example: D1 from SanFran is paired with D1 on SanJose

   Type

   ```
   ADD REMOTE RCS_D1 D1 SANJOSE\D1
   ADD REMOTE RCS_D2 D2 SANJOSE\D2
   ```

   Important
   Do not perform this step on the SanJose units.

3. View the normalization percent for the remote copies.

   Type

   ```
   SHOW REMOTE FULL
   ```

   Note
   The remote copy sets will not be shown at the SanJose (target) site unless there is a failover.

**********SANFRAN**********

Creating Log Units and Association Sets

In the event of a link failure, disk operations between the host and subsystem on SanFran (initiator) will continue and changes will be recorded in this log. When the link is restored, a full synchronization between the SanFran (initiator) and SanJose (target) systems will not be necessary. Only the data referenced in the write-history log will be exchanged.

In this exercise, disks 40000 and 60000 are used as a mirrorset for the log disk. The log unit name is D3. The association set name is AS_SQL. The remote copy sets used in this scenario are RCS_D1 and RCS_D2.

Creating a Log Unit

1. Create a mirrorset for the log disk.

   Type

   ```
   ADD MIRROR LOG1 DISK40000 DISK60000
   ```

2. Initialize the mirrorset with the following CLI command:

   Type

   ```
   INIT LOG1
   ```

   Important
   The drives for this log are only on the SanFran (initiator) side.

3. Assign a unit (LUN) to the container you just created.

   Type

   ```
   ADD UNIT D3 LOG1
   ```

4. Prepare D3 for inclusion in the association set. Log entries will be used to synchronize the copy sets, so all log entries must be written to disk immediately, not stored in cache. To ensure that this occurs, disable write-back caching for the log unit.

   Type

   ```
   SET D3 DISABLE_ACCESS_PATH=ALL
   SET D3 NOWRITEBACK_CACHE
   ```

5. Ensure that the commands are accepted.

   Type

   ```
   SHOW UNITS FULL
   ```

**********SANFRAN**********

Create an Association Set

An association set refers to the group containing a log disk and the remote copy sets that use it. Create an association set that includes D3 (the log just created), D1 (the data store for the SQL database), and D2 (the SQL database log). Name this association set *AS_SQL*.

If the link between SanFran and SanJose fails, transactions to D1 and D2 will be logged in the write-history log unit.

1. Create the association set and include the application data store as the first member.

   Type

   ```
   ADD ASSOCIATIONS AS_SQL RCS_D1
   ```

2. Add the application log file as the second member of the association set:

   Type

   ```
   SET AS_SQL ADD=RCS_D2
   ```

3. Assign D3 as the log unit to the AS_SQL association set.

   Type

   ```
   SET AS_SQL LOG_UNIT=D3
   SHOW AS_SQL
   ```

List Remote Copy Sets and Associations Sets

Type

```
SHOW REMOTE FULL
```

Write down the remote copy set and association set information from this display.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

**********SANFRAN**********

At SanFran (Initiator)

1. View the connections on SanFran and rename them.

   Type

   ```
   SHOW CONN
   RENAME !NEWCONNxx IT1
   RENAME !NEWCONNyy IB1
   ```

2. Enable the connections on SanFran (initiator).

   Note
   When the Enable_Access_Path command is executed, a warning message about other hosts will display. This message is correct; access has been enabled for other hosts to this unit. Acknowledge that you have read the warning message and continue.

   Type

   ```
   SET D1 ENABLE_ACCESS_PATH=IT1,IB1
   SET D2 ENABLE_ACCESS_PATH=IT1,IB1
   ```

3. Log in to the host.

   Important
   Update your script files. Type *copy the \scripts folder to c:\scripts.* Allow files to be overwritten if necessary.

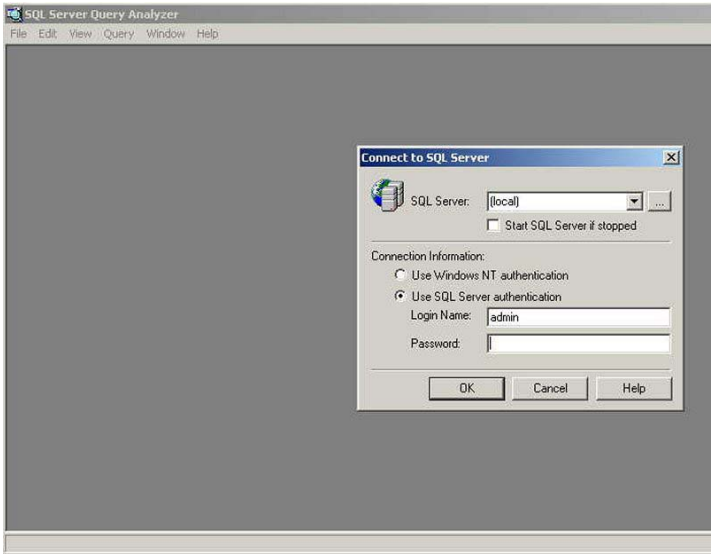
4. Run *My Computer* → *Manage* → *Disk Management* and write signatures to the new drives. Assign fixed drive letters F: and Z: to the two new drives.

   Important
   The scripts written for this lab assume the use of the F: and Z: drives. If you assign other drive letters, the SQL scripts will fail.

**********SANFRAN**********

Testing the Configuration at SanFran (Initiator)

1. Using Windows Explorer, find the batch file *c:\scripts\CreateDB_DRM.bat*. Double-click *c:\scripts\CreateDB_DRM.bat* to execute the batch file.
2. Locate the executable *iSQLw.exe* and double-click *iSQLw.exe to* execute the file.



3. Log in with the admin user ID and no password. Use the defaults shown in the preceding graphic for the other parameters.
4. From the same directory, select *File* → *Open* → *CreateOriginal_DRM.sql*.
5. The SQL statement in this query creates a simulation of data entry in a database application.
6. Click the green arrow (run) icon in the menu bar to execute the SQL script.
7. While the database application is active:
   a. Disconnect the active ISL (indicated by the activity light to that connection on the switch). After a few minutes, the controllers will recognize a path failure and transfer to the other fabric (switch).

      What is the effect on the application?

      .....

   b. Disconnect the remaining ISL. After a few minutes the SanFran (initiator) subsystem will begin writing information to the log. When the connection is restored, the initiator will resume the copy operation using the information that was stored on the logs.

      What is the effect on the application?

      .....
8. Reconnect the ISLs to the original switches and fabric.

**********SANFRAN**********
*****

Managing Site Failure

WARNING
Ensure that normalization of the remote copy sets is complete **before** beginning this lab. Enter the show remote full command to view the normalization status.

**********SANFRAN**********

Exercise 1: Starting the Application

In this exercise, you will start a simulated database application then failover to the target and restart the application. If the database application is already started, skip to *Exercise 2*.

Note
Your instructor will point you to the files necessary to start this application data simulation if the scripts on not in *c:\scripts*.

1. Open *iSQLw.exe.*
2. Log in with the *admin* user ID and no password.
3. From the same window, select *File* → *Open* → *CreateOriginal_DRM.sql*.

   The SQL statement in this query creates a simulation of data entry in a database application.
4. Click the green arrow (run) icon in the menu bar to execute the SQL script.
5. Leave the *iSQLw.exe* window open with the script running.

**********SANFRAN**********

Exercise 2: Initiating a Site failure

At the SanFran (Initiator) SIte

You have experienced an unplanned loss of the initiator site (SanFran). The loss could have been caused by a power failure or other event that did not damage initiator site hardware. The duration of the outage at the initiator is unknown. The DRM hardware components (hosts, controllers, and switches, for example) at the initiator site will remain intact.

You will perform a failover to the target site. When the power is returned to the initiator site and the system is back online, you will perform a full failback to the initiator site (SanFran).

> **!** **Important**
> Because an actual site failure would include both the host and the subsystem at SanFran, you must first shutdown the host at SanFran so that it no longer has access to the subsystem.

To stop communication between the host and the storage subsystem, power off the host server at the initiator SanFran (simulated power failure).

> **Note**
> In a normal full power failure at the initiator site (SanFran), the storage systems also would lose power. However, for of this exercise, we will assume that there is a loss of power to the storage but leave the storage systems running.

**********SANJOSE**********

At SanJose (Recovery System)

! Important

- The SITE_FAILOVER command must be issued for each remote copy set so that if SanFran comes back online, it will see another initiator (SanJose in this case) for the remote copy sets and will not start to spread its WWID on the fabric. This prevents it from being available as a SCSI target.
- After ensuring that SanFran does not have access to the storage system, allow access through the paths connecting the SanJose storage system to the HBAs on the SanJose server.

1. Disable communications on Port 2. Do not disconnect the ISLs from the switches.

   Type:

   ```
   SET THIS PORT_2_TOPOLOGY=OFFLINE

   SET OTHER PORT_2_TOPOLOGY=OFFLINE
   ```

2. Verify that the connection is offline.

   Type:

   ```
   SHOW THIS

   SHOW OTHER
   ```

   What is the status of the PORT_1_TOPOLOGY and PORT_2_TOPOLOGY?

   .....

3. Issue the SITE_FAILOVER command for each remote copy set.

   Type

   ```
   SITE_FAILOVER SANFRAN\RCS_D1

   SITE_FAILOVER SANFRAN\RCS_D2
   ```

   What occurred?

   .....

4. Verify that all remote copy sets now refer to SanJose as the initiator and SanFran as the target.

   Type

   ```
   SHOW REMOTE FULL
   ```

**********SANJOSE**********

5. Remove the targets associated with SanFran in case SanFran where to recover.

```
SET RCS_D1 REMOVE=SANFRAN\D1
SET RCS_D2 REMOVE=SANFRAN\D2
```

6. Verify that you have removed the targets.

   Type

```
SHOW REMOTE FULL
```

   What is the difference between this list and the one in step 4?

   .....

   .....

   .....

7. Refer to your record of the `SHOW REMOTE FULL` command output that details the original initiator configuration (step 4). Using the output as a reference, create association sets to duplicate all of the association sets that were on the initiator. Do not create a log disk.
8. Power on the server at SanJose.
9. After the server boots, rename the connections to the SanJose (recovery) server HBAs.

   Type

```
RENAME !NEWCONNxx TT1
RENAME !NEWCONNyy TB1
```

10. Grant access for the SanJose server to the SanJose storage for every unit on the SanJose controller pair. If you do not know the connection names, issue a `SHOW CONNECTION` CLI command.

> **Note**
> When you issue these commands, you will receive the warning message noting that other hosts enabled for these units. Acknowledge this warning and continue.

   Type

```
SET D1 ENABLE=TT1,TB1
SET D2 ENABLE=TT1,TB1
```

**********SANJOSE**********

11. Log in to the SanJose computer as Administrator.
12. Right-click *My Computer* and select *Manage*. Rescan disk drives and verify that the drives (LUNs) are now visible on SanJose. Also verify that the drives are assigned the same drive letters they were assigned at SanFran.
13. Start the SQL server.
14. From the c:\scripts directory, execute the batch file *AttachDB.bat*.
15. Open *iSQLw.exe.*
16. Log in with the *admin* user ID and no password.
17. In iSQLw, select *File* → *Open* → *ShowCount.sql*.
18. Click the green arrow (run) icon in the menu bar to execute the SQL script.

    What number displays in the Result tab?

    .....
19. In iSQLw, select *File* → *Open* → *ShowData.sql*.
20. Maximize the iSQLw window.
21. Click the green arrow (run) icon in the menu bar to execute the SQL script.

    Can you tell where the data originated?

    .....

    (Hint: It is part of the record.)
22. Select *File* → *Open* → *CreateData_DRM_Target.sql*.
23. Click the green arrow (run) icon in the menu bar to execute the SQL script.

This ends the site failover procedure to the remote site.

Managing Site Failback

Before performing a full failback, verify that your initiator controller configuration is the same as your target controller configuration.

Compare the status of the controllers, association sets, remote copy sets, units, and connections at the target site with those at the initiator site. Full failback consists of:

- Initiator site preparation
- Target site copy data
- Initiator site return control
- Target site restoration
- Initiator site restoration of target connections

Exercise 1: Preparation

**********SANFRAN**********

Initiator Site Preparation (SanFran)

1. Power up the controllers, if necessary.
2. Check all units for lost data.

   Type

   ```
   SHOW UNITS FULL
   ```

   Which units need to be cleared?

   .....

   How could you tell which ones had errors (if any)?

   .....

   (Hint: What is the state of the unit?)

3. If there is lost data, clear it for each applicable unit.

   Type

   ```
   CLEAR_ERRORS unitname LOST_DATA (if necessary)
   ```

   Repeat this step for any units that had errors.

4. If no errors were found in step 2, skip to step 5. Otherwise, enter the following command to verify that all errors have been corrected.

   Type

   ```
   SHOW UNITS FULL
   ```

   Were all units cleared?

   .....

5. Disable access to the storage unit.

   Type

   ```
   SET D1 DISABLE_ACCESS IT1,IB1
   SET D2 DISABLE_ACCESS IT1,IB1
   ```

**********SANFRAN**********

6. Verify that access has been disabled.

   Type

   ```
   SHOW UNITS FULL
   ```

7. If necessary, turn off write-history logging for each association set.

   Type

   ```
   SET AS_SQL NOLOG
   ```

   Repeat this command for all association sets.

8. Delete all association sets.

   ```
   DELETE AS_SQL
   ```

   Repeat this command for all association sets.

9. Delete all remote copy sets.

   Type

   ```
   DELETE RCS_D1
   ```

   Repeat this command for all remote copy sets.

**********SANJOSE**********

Target Copy Data Procedure (SanJose)

1. Reenable host Port 2 on both controllers.

   Type

   ```
   SET THIS PORT_2_TOPOLOGY=FABRIC
   SET OTHER PORT_2_TOPOLOGY=FABRIC
   ```

3. Verify that the ports have been reenabled.

   Type

   ```
   SHOW THIS
   SHOW OTHER
   ```

4. Add the target back to the remote copy sets of the initiator.

   Type

   ```
   SET RCS_D1 ADD = SANFRAN\D1
   SET RCS_D2 ADD = SANFRAN\D2
   ```

   This step initiates the failback copy and begins normalization.

5. Check the progress of the normalization (copy) cycle.

   Type

   ```
   SHOW REMOTE FULL
   ```

**********SANJOSE**********

6. In iSQLw.exe, click the red stop icon in the menu bar to stop execution of the script.
7. Close the iSQLw.exe window.
8. In the SQL Server Service Manager window, stop SQL Server.
9. Shutdown the SanJose server.
10. On the SanJose storage system, disable access to the storage by the remote server. This prevents problems that could occur if the remote server comes back online.

    Type

    ```
    SET D1 DISABLE=TT1,TB1
    SET D2 DISABLE=TT1,TB1
    ```

    Type

    ```
    SHOW UNITS FULL
    ```

    What is the access for each of the units?

    .....

    .....

! Important

Continue to monitor the normalization progress using the `SHOW REMOTE FULL` command. Wait until all remote copy sets are 100% normalized before proceeding to the next step in this lab. This indicates that all copy cycles are finished.

Exercise 2: Performing Failback

**********SANFRAN**********

SanFran (Initiator) Return Control Procedure

1. Disable communications on Port 2.

   Type:

   ```
   SET THIS PORT_2_TOPOLOGY=OFFLINE
   SET OTHER PORT_2_TOPOLOGY=OFFLINE
   ```

2. Verify that the connection is offline.

   Type:

   ```
   SHOW THIS
   SHOW OTHER
   ```

3. Issue the `SITE_FAILOVER` command for each remote copy set.

   Type

   ```
   SITE_FAILOVER SANJOSE\RCS_D1
   SITE_FAILOVER SANJOSE\RCS_D2
   ```

   What occurred?

   .....

**********SANJOSE**********

SanJose (Target) Restore Procedure

Repeat this command for all association sets.

1. Delete all remote copy sets.

   Type

   ```
   DELETE RCS_D1
   ```

   Repeat this command for all remote copy sets.

**********SANFRAN**********

SanFran (Initiator) Restoration of Target Connections

1. Reenable host Port 2 on both controllers.

   Type

   ```
   SET THIS PORT_2_TOPOLOGY=FABRIC
   SET OTHER PORT_2_TOPOLOGY=FABRIC
   ```

2. Re-create the association sets.

   Type

   ```
   ADD ASSOCIATIONS AS_SQL RCS_D1
   SET AS_SQL ADD=RCS_D2
   SHOW AS_SQL
   ```

3. Enable access to the SanFran storage by the SanFran server.

   Note
   When you issue the following command, you may receive the message noting that hosts enabled for these units. Acknowledge the warning and continue.

   Type

   ```
   SET D1 ENABLE=IT1,IB1
   SET D2 ENABLE=IT1,IB1
   ```

4. Verify that you have granted access to every unit (LUN) that is part of a remote copy set (RCS).

   Type

   ```
   SHOW UNITS FULL
   ```

   Important
   Remember to check the error_mode on every remote copy set on SanFran. Change the error mode to *NORMAL* or *FAILSAFE* (`SET <RCSName> ERROR = FAILSAFE [NORMAL]`).

**********SANFRAN**********

5. Reboot the SanFran server and log in as Administrator. Select *My Computer* → *Manage* → *Disk Management*. Rescan and verify that you have access to all the drives (LUNs).

6. Open SQL Server Service Manager from the system tray. Click *Stop*.
7. Wait for the server to stop, then click *Start/Continue*.
8. Open iSQLw.exe.
9. Log in using with user id *admin* and no password. Use the defaults for any other parameters.
10. In iSQLw.exe, select *File* → *Open* → *ShowCount.sql*.
11. Click the green arrow (run) icon in the menu bar to execute the SQL script.

    Was there a difference between this count and the one recorded earlier?

    .....
12. Maximize the iSQLw.exe window.
13. In iSQLw.exe, select *File* → *Open* → *ShowData_DRM_Target.sql* (c:\scripts directory).

    Can you tell where the data originated?

    .....

    (Hint: It is part of the record)

This ends the Site Failback procedure.

SanFran is now the initiator again.

The DRM Lab is now complete.

Let your instructor know that you are finished.

scripting hp StorageWorks data replication manager

lab 5

Objectives

The Widget company was very impressed with the ability of Data Replication Manager (DRM) to replicate the company's data to the San Jose facility. After further review of the abilities of DRM, the IT managers of Widget have decided that while their data needs to be highly available, they are more concerned about the integrity of the data. They would prefer to use the Failsafe error mode for their DRM configuration, and to keep a spare server in San Jose that could be quickly brought up to host their database.

Because the speed of recovery is important to them, they would also like you to configure scripts that will facilitate the resumption of operations.

Overview

Usually, to perform failover, failback, or a resumption of operations, the manual issuance of a complex series of Command Line Interpreter (CLI) commands is required. The use of scripts reduces the number of manual commands that have to be issued. The appropriate CLI commands can be run in a batch file..

After completing this lab, you should be able to explain:

- How to obtain and install the necessary program files.
- How to customize the following files for a DRM configuration:
  - Configuration generation batch files.
  - Target controller configuration files.
  - The application action list.
- How to run the failover, failback, and resumption of operation batch files.

**********SANFRAN**********

Changing the Error Mode

For the purposes of this lab, the error mode that will be used is the Failsafe error mode. Complete the following steps to change the error mode from normal to failsafe.

1. Turn off write history logging, if enabled.

   Type:

   ```
   SET AS_SQL NOLOG_UNIT
   ```

2. Use the following CLI command to verify that the association sets have no log unit.

   Type:

   ```
   SHOW ASSOCIATION FULL
   ```

3. Delete the configured association set.

   Type:

   ```
   DELETE AS_SQL
   ```

4. Set the error mode of the remote copy sets to failsafe.

   Type:

   ```
   SET RCS_D1 ERROR_MODE = FAILSAFE
   SET RCS_D2 ERROR_MODE = FAILSAFE
   ```

5. Create the association set and include the application data store as the first member.

   Type:

   ```
   ADD ASSOCIATIONS AS_SQL RCS_D1
   ```

6. Add the application log file as the second member of the association set.

   Type:

   ```
   SET AS_SQL ADD=RCS_D2
   ```

**********Both Sites**********

Scripting Software Installation

The following software components are required to prepare a server for script operation:

- DRM Scripting Kit
- Perl interpreter
- Command Scripter

These software components must be installed on each host at the initiator and target sites that will use scripting.

DRM Scripting Kit

1. Copy the DRM scripting kit self-extracting file into the c:\scripts directory.
2. From Windows Explorer or a command line prompt, double-click or execute the installation file. The kit files self-extract into the c:\scripts directory.
3. Verify that the subdirectories BAT, BIN, CONFIG, LOG, and TMP are created in the c:\scripts directory.
4. Add an environmental variable named %CLONE_HOME% to set the default directory of the scripts.
   a. From the Windows desktop, click *Start* → *Settings* → *Control Panel*.
   b. Double-click *System*.
   c. Click *Advanced* → *Environment Variables*.
   d. In the System Variables section, click *New*.
   e. In the dialog box, type *CLONE_HOME* in the Variable Name field. In the Variable Value field, enter *c:\scripts*.
   f. Click *OK*.

Perl Interpreter

A Perl interpreter is necessary to execute the Perl scripts, and must be installed on each server that runs the scripts. For the Windows NT/Windows 2000 platform, the interpreter is a separately installed component. ActivePerl is one interpreter that can be downloaded for free and used to run the scripts.

1. Locate the Perl interpreter supplied by your instructor.
2. Follow the installation instructions for the interpreter.

**********Both Sites**********

Command Scripter

The Command Scripter must be installed on the initiator and target servers. The following procedure installs the Command Scripter:

1. Obtain the location of the installation files from your instructor. Execute *setup.exe.*
2. From the Welcome screen, click *Next*.
3. The license agreement displays. Click *Yes* to accept the license agreement.
7. Accept the default or choose a destination for the program installation. Click *Next*.
8. Click *Finish*. A Command Scripter program icon is added to the Programs menu.
9. Install the Command Scripter 1.0A or later update.
10. Copy cmdscript.exe to c:\scripts\bin.

**********SanFran**********

Creating SCSI-3 Individual Generation Batch Files

1. Modify the *gen_ex.bat* file, located in the *C:\SCRIPTS\BAT* directory, to create an initiator configuration generation file for the initiator site. Use a text editor and make the necessary modifications using the following syntax:

   ```
   Perl -I %CLONE_HOME% %CLONE_HOME%\bin\generate_cfg.pl
   com=cs RemoteCopyName HSG Serial #:
   ```

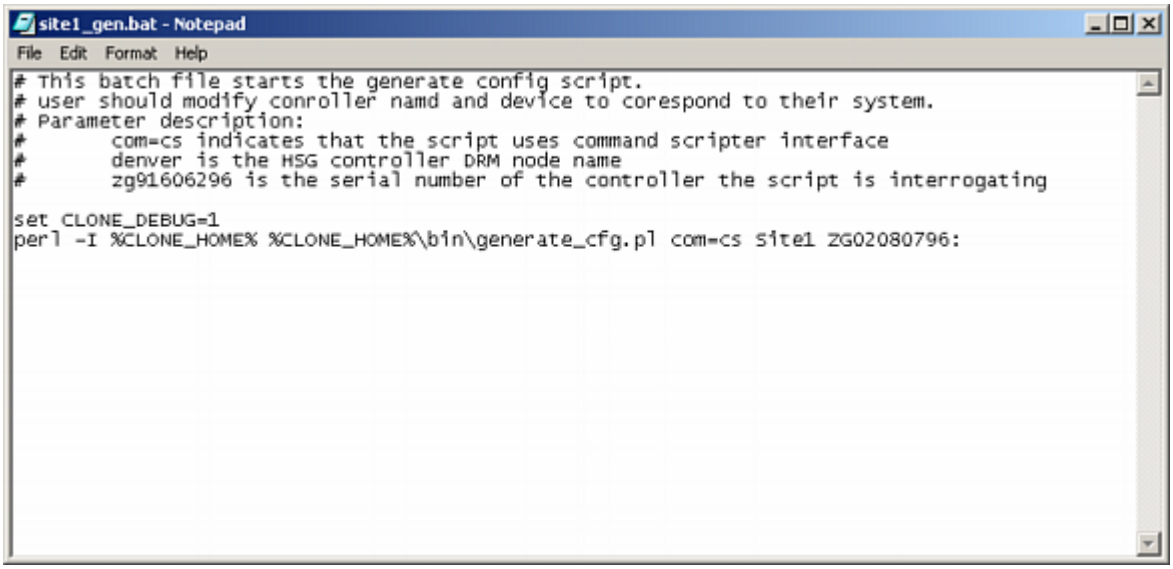
   RemoteCopyName identifies the DRM controller (remote copy) name of the **initiator** subsystem (for example, SanFran). The remote copy name can be obtained by running a *SHOW THIS* command from the controller.

   Edit the gen_ex.bat file to look like the following :

   ```
   Perl -I %CLONE_HOME% %CLONE_HOME%\bin\generate_cfg.pl com=cs SanFran
   Z603004687:
   ```

   Note

   You would replace the controller serial number in the example above to your *THIS* controller's serial number.



3. Save the edited initiator configuration generation batch file into the %CLONE_HOME%\BAT subdirectory with the name *SanFran_gen.bat.*

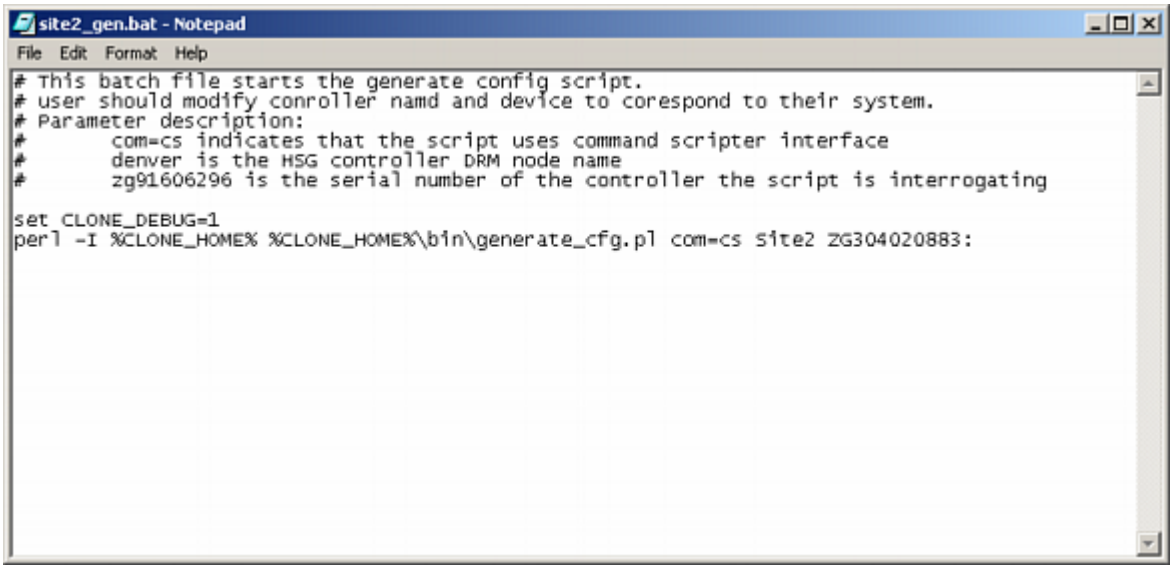
11. Modify the *gen_ex.bat* file again to create a target configuration generation file for the initiator site. The syntax is:

```
Perl -I %CLONE_HOME% %CLONE_HOME%\bin\generate_cfg.pl
com=cs RemoteCopyName Device:
```

RemoteCopyName identifies the DRM controller (remote copy) name of the target subsystem (for example, SanJose).

Edit the gen_ex.bat file to look like the following :

```
Perl -I %CLONE_HOME% %CLONE_HOME%\bin\generate_cfg.pl com=cs SanJose
ZN304020883:
```



12. Save this batch file in the BAT subdirectory with the name *SanJose_gen.bat*.

**********SanJose**********

1. Repeat the previous steps to create initiator and target configuration generation batch files for the target site. Save these batch files in the BAT subdirectory on the target host using the same naming convention used previously.

**********Both Sites**********

Running Configuration Generation Files

After creating an initiator and target configuration generation file for each controller subsystem at each site, execute each file on the initiator host and on the target host. For example, the initiator configuration generation file for controller *SanFran* is run from the initiator site, and a configuration generation file for controller *SanFran* is run from the target host. Remember that any time the controller configuration changes, these generation files must be run again to create new controller configuration files.

The configuration generation files run a Perl script called *generate_cfg.pl*. When this script runs:

- Many *show* commands are sent to the applicable HSG80 controller. The script creates a controller configuration file based on the received responses.
- This resulting configuration file framework is named by the script in the format *ControllerName.cfg*.

Follow these steps to run the configuration generation files:

1. In Windows Explorer, locate the configuration generation batch files (*SanFran_gen.bat, SanJose_gen.bat*) in the *%CLONE_HOME%\BAT* directory.
2. *Double-click or run* the batch file for the first controller.
3. Run the configuration generation batch file for each initiator and target controller on the initiator and target hosts.

   For example, the *SanFran_gen.bat* we created above is run and creates a configuration file called *SanFran.cfg* and places it in the *CONFIG* subdirectory of the *CLONE_HOME* directory.

**********Both Sites**********

Controller Configuration File Customization

The configuration files that are created after running the generation batch files, and placed in the CONFIG subdirectory, represent a picture in time of the controller configuration. The information in these files enables the Perl scripts to issue the correct commands. The sections in these files have names like ASSOCIATIONSET, CONNECTIONS, CONTROLLER, and so on.

After the configuration files have been generated, you will have files for both the initiator and target controllers. Please note that:

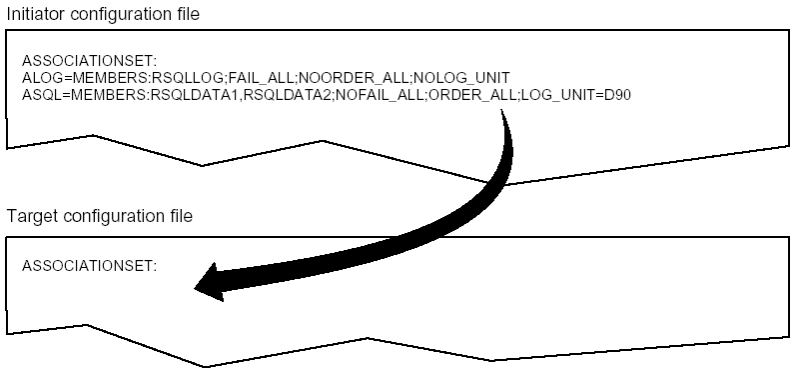
- The configuration files for the initiator controllers are complete and do not have to be modified.
- The configuration files for the target controllers must be modified each time they are created, to put them into a state that should exist after failover.
- The configuration file for a controller must be recreated by rerunning the generation batch file every time there are changes made to the configuration of that controller.

**********Both Sites**********

Target Controller Configuration File Customization

The target controller configuration files are built by running configuration generation batch files that execute the *generate_cfg.pl* script. However, these files require additional information to allow the target site to assume the initiator role after failover.

Association Set Section

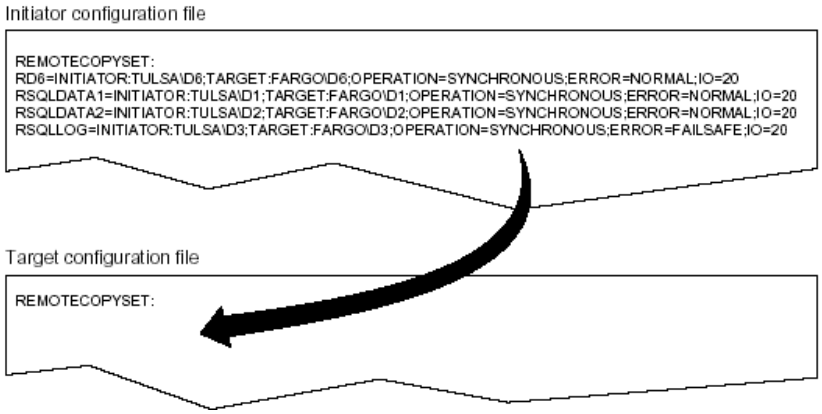


This section exists in the initiator configuration file, but not in the target configuration file, because association sets do not exist on the target site when the script is executed.

To make the necessary changes:

1. Using a text editor, copy the information from the initiator configuration file into the target configuration file.

Remote Copy Set Section



This is another section that does not exist in the target configuration file because the information is not available when the script is run.

2. Using a text editor, copy information from the corresponding initiator configuration file into the target file.

**********Both Sites**********

Connections Section

This section in the configuration file specifies which server has access to the controllers. Only the DRM initiator connections will have been inserted in this section by the remote copy set LUNs. You must modify this section to enable the target-site servers access to these controllers following a site failover. To do this, modify the target configuration file with the names of the desired server connections. Spaces between the connection names are not allowed.

For example, TT1 and TB1 are target-site server connections to be given access to the controllers.

3. Modify the SanJose.cfg (Target) file with a text editor resulting with the section looking like the following:

```
CONNECTIONS:
D1=SanFranA,SanFranB,SanFranC,SanFranD,TT1,TB1
D2=SanFranA,SanFranB,SanFranC,SanFranD,TT1,TB1
```

NOTE: If an ***ACCESS:,*** statement appears in the CONNECTIONS: of units D1 or D2 remove the ***ACCESS:,*** portion only. Make certain that you never have more than one space between the « , » and the next connection name.

Target File (SanJose.cfg) Example :

```
CONNECTIONS: (BEFORE !)
D1=ACCESS:,SanFranA,SanFranB,SanFranC,SanFranD,TT1,TB1
D2=ACCESS:,SanFranA,SanFranB,SanFranC,SanFranD,TT1,TB1
```

```
CONNECTIONS: (AFTER !)
D1=SanFranA,SanFranB,SanFranC,SanFranD,TT1,TB1
D2=SanFranA,SanFranB,SanFranC,SanFranD,TT1,TB1
```

Modify (if necessary) the SanFran.cfg (Intiator) file with a text editor resulting with the section looking like the following:

```
CONNECTIONS:
D1=SanJoseA,SanJoseB,SanJoseC,SanJoseD,IT1,IB1
D2=SanJoseA,SanJoseB,SanJoseC,SanJoseD,IT1,IB1
```

NOTE: If an ***ACCESS:,*** statement appears in the CONNECTIONS: of units D1 or D2 remove the ***ACCESS:,*** portion only. Make certain that you never have more than one space between the « , » and the next connection name.

Intiator File (SanJose.cfg) Example :

```
CONNECTIONS: (BEFORE !)
D1=ACCESS:,SanJoseA,SanJoseB,SanJoseC,SanJoseD,IT1,IB1
D2=ACCESS:,SanJoseA,SanJoseB,SanJoseC,SanJoseD,IT1,IB1
```

```
CONNECTIONS: (AFTER !)
D1=SanJoseA,SanJoseB,SanJoseC,SanJoseD,IT1,IB1
D2=SanJoseA,SanJoseB,SanJoseC,SanJoseD,IT1,IB1
```

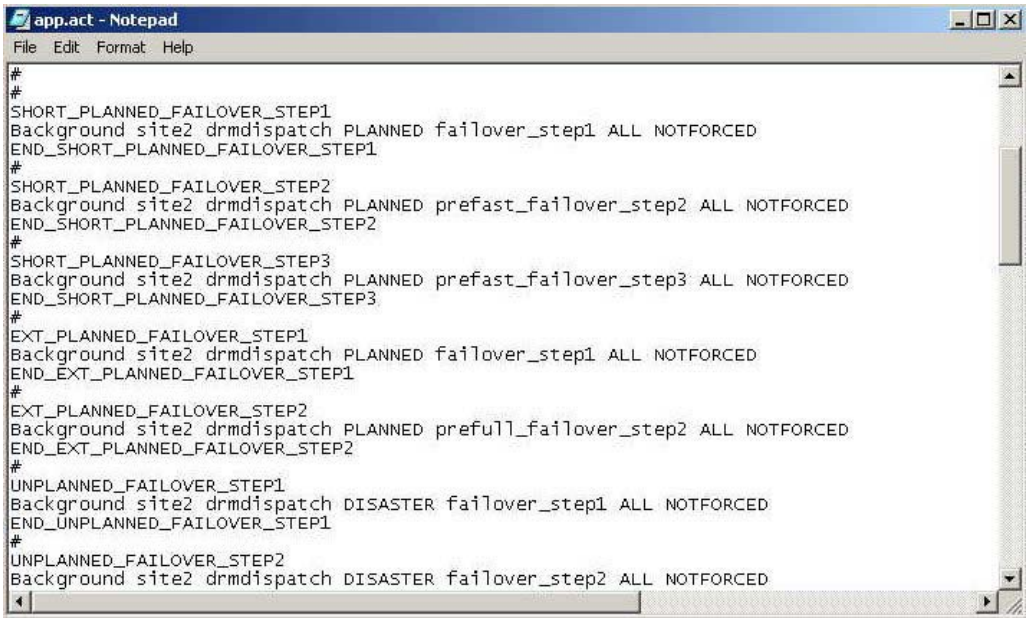
Maximum Read/Write Transfer Size Section

When it was created, default values were loaded into the target configuration file that do not correspond to the values in the initiator configuration file. Change these values to match those of the initiator configuration file. Ensure that the units being modified are mapped to the correct remote copy sets.

13. With a text editor, modify the values in the target configuration file to match the values of the initiator.

**********Both Sites**********

Application Action List Customization



During installation, the default application action list (*app_ex.act*) was extracted from the DRM Scripting Kit and placed in the CONFIG subdirectory of CLONE_HOME. It provides a basic structure that you must customize using the procedures below.

Customizing the Application Action List

1. Rename the *app_ex.act* file to *app.act* in the *CONFIG* directory.
2. With a text editor, open the *app.act* file.
3. Delete one row from each action in the list.

   Populate the number of actions to correspond with the number of DRM subsystems. The number of initiator-target subsystems will match the number of entries for each action. For our lab, one DRM subsystem will comprise one entry under each action.

```
SHORT_PLANNED_FAILOVER_STEP1
Background fargo drmdispatch PLANNED failover_step1 ALL NOTFORCED
Background denver drmdispatch PLANNED failover_step1 ALL NOTFORCED
END_SHORT_PLANNED_FAILOVER_STEP1
```

14. For each entry within a failover or failback action section, modify the controller name to that of the **target** controller name for each DRM initiator-target pair.

```
SHORT_PLANNED_FAILOVER_STEP1
Background SanJose drmdispatch PLANNED failover_step1 ALL NOTFORCED
END_SHORT_PLANNED_FAILOVER_STEP1
```

15. For each entry containing failsafe-lock actions, modify the controller name to that of the **initiator** controller name for each DRM initiator-target pair.

    Sections to be modified are:

    - **SET_ERROR_NORMAL_OPERATION**
    - **SET_ERROR_CONFIGURED_OPERATION_STEP1**
    - **SET_ERROR_CONFIGURED_OPERATION_STEP2**

16. Save the *app.act* file.

Unplanned Site Failover with Full Failback Procedure

These procedures are used when there is an unplanned loss of the initiator site with a full failback to the existing hardware. The procedures are:

- Running the Unplanned Failover Batch File Procedure
- Target Host Setup Procedure
- Running the Full Failback Batch Files Procedure
- Initiator Site Cleanup Procedure

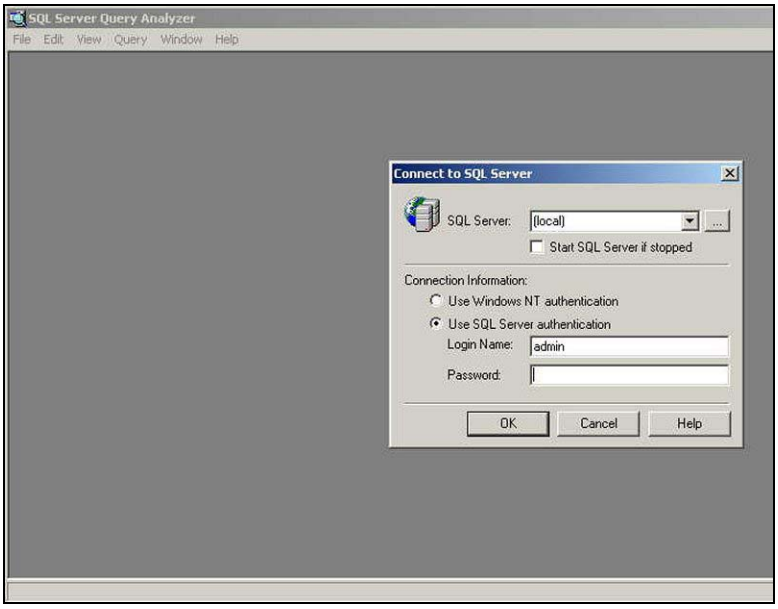
**********SANFRAN**********

Exercise 1: Starting Application

In a business environment, one need to replicate data would be the need to continue using a database after a site failure. In this exercise, we will start a simulated database application then failover the to the target and restart the application.

> **Note**
> Your instructor will point you to the files necessary to start this application data simulation if the scripts on not in *c:\scripts*.

1. Using Windows Explorer, find the executable *C:\MSSQL7\BINN\ISQLW.exe*. Double-click *iSQLw.exe*.



2. Log in using with user id *admin* and no password. Use the defaults shown above for the other parameters.
3. Select *File* → *Open* → *CreateOriginal_DRM.sql*.

   The SQL statement in this query creates a simulation of data entry in a database application.
4. Click the green arrow (run) icon in the menu bar to execute the SQL script.
5. Leave the iSQLw window open with the script running.

**********SANFRAN**********

Exercise 2: Site failure

At SanFran (Initiator)

You have experienced an unplanned loss of the initiator site (SanFran). The loss could have been caused by a power failure or other event that did not damage initiator site hardware. The duration of the outage at the initiator is unknown. The DRM hardware components (hosts, controllers, switches, for example) at the initiator site will remain intact.

You will perform a failover to the target site. When the power is returned to the initiator site and it is back online, you will perform a full failback to the initiator site (SanFran).

> **! Important**
> Since an actual site failure would include **both** the host **and** the subsystem at SanFran, you must first shutdown the host at SanFran so that it no longer has access to the subsystem.

First, stop the SQL script and make sure that there is no communication between the host and the storage subsystem.

1. Power off the host server at the initiator SanFran (simulated power failure).

> **Note**
> In a normal full power failure at the initiator site (SanFran), the storage systems would lose power as well. However, for the purpose of this exercise we will assume a loss of power to the storage, but we will leave the storage systems running.

**********SANJOSE**********

Exercise 3 - Running the Unplanned Failover Batch File Procedure

1. Open a command prompt window on the target host.
2. Verify that the script server can communicate with the intiator (SanFran) controller via Command Scripter.

   For SCSI-3, use the command:

   ```
   \scripts\bin\cmdscript -n Z60300487 "show this"
   ```

   Note
   You would replace the controller serial number in the above example with the serial number of your *THIS* controller.

   You should expect a normal SHOW THIS response.
3. Check the error mode, initiator state, and target status of all remote copy sets with the CLI command:

   ```
   SHOW REMOTE_COPY_SETS FULL
   ```

   Note
   Full syntax is required for commands issued during a Command Scripter session.

```
----------------------------------------------------------------
RCS_D1 remote copy D1 AS_SQL
Reported LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003E
Switches:
OPERATION_MODE = SYNCHRONOUS
ERROR_MODE = FAILSAFE
FAILOVER_MODE = MANUAL
OUTSTANDING_IOS = 20
Initiator (SANFRAN\D1) state:
INOPERATIVE
Unit failsafe locked
Target state:
SanJose\D1 is COPYING 0% complete
```

4. Change to the BAT subdirectory in the CLONE_HOME directory.

17. Run the *hsg_fo.bat* file.

18. You will see a message asking what type of failover to run. Enter **u** for an unplanned failover.

19. You will see a confirmation message that asks you to confirm that an unplanned failover is desired. Enter **y** for yes.

20. If this is the first time the batch file is run, or you have deleted the .RC file, you are prompted to select a verbose or condensed reporting display. Enter **v** for verbose.

21. When an operation completion status result is displayed, continue the fail over procedure at the target site with the “Target Host Setup Procedure.”

**********SANJOSE**********

Exercise 4 - Target Host Setup Procedure

1. To verify that failover completed successfully, issue this CLI command:

   ```
   SHOW REMOTE_COPY_SETS FULL
   ```

   The output shows the status of remote copy sets. Be sure the units listed under Initiator State are at the target site.

2. To verify that the target hosts can connect to the LUNs, use this command:

   ```
   SHOW UNITS FULL
   ```

   In the Access field of the display, all units that are used by remote copy sets should show that the target hosts connections are enabled. This should also show the initiator controller connections.

3. Allow the target host to recognize new units. If you *have not* changed the UNIT_OFFSET of any host connections since the hosts have been booted, you do not need to reboot the target site hosts.

4. Open Computer Management and click Disk Management.

22. After *Disk Management* has initialized, go to the *Action Menu* and click *Rescan Disks*. All of the failed over units should appear in the right-hand pane. If Secure Path is not installed correctly, you will see each unit twice.

    If you *have* changed the UNIT_OFFSET of any host connections, you must reboot that host. You should be able to see all of the units in Disk Management.

**********SANJOSE**********

Exercise 5 - Target Host SQL Recovery

1. Locate *attachDB.bat* in the c:\scripts directory of your remote site. Double-click *attachDB.bat*.
2. Open SQL Enterprise Manager. Verify that the *PseudoApplicationDB* database has been attached.

   If the failover has cause the database to be suspect (error from SQL Server),

   a. Stop and restart the SQL Server service

   b. If you still have a problem, truncate the log for that database

> **!** **Important**
> In a customer environment a suspect database would require a more robust recovery method.

3. Locate *iSQLw.exe* from your remote site. Double-click *iSQLw.exe*.
4. Log in using user id *admin* and no password. Use the defaults for any other parameters.
5. In iSQLw, select *File* → *Open* → *CreateData_DRM_Target.sql*.
6. Click the green arrow (run) icon in the menu bar to execute the SQL script.
23. After a few seconds, stop the script.
24. In iSQLw, select *File* → *Open* → *ShowCount.sql*.
25. Click the green arrow (run) icon in the menu bar to execute the SQL script.

    Write down the number displayed in the Result tab.

    .....
26. In iSQLw, select *File* → *Open* → *ShowData.sql*.
27. Maximize the iSQLw window.
28. Click the green arrow (run) icon in the menu bar to execute the SQL script.

    Can you tell where the data originated? (Hint: It's part of the record)

    .....
29. Locate *detachDB.bat* in the c:\scripts directory of your remote site. Double-click *detachDB.bat*.
30. Using SQL Enterprise Manager, verify that the database has been detached. It may require that the manager is closed and re-opened to refresh the database list.

**********SANFRAN**********

Exercise 6 - Running the Full Failback Batch Files Procedure

1. Bring the initiator host back online.
2. Open a command prompt window on the initiator host.
3. Verify that the script server can communicate with the initiator controller via Command Scripter.

   For SCSI-3, use the command:

   ```
   \scripts\bin\cmdscript -n Z600300487 "show this"
   ```

   Note
   You would replace the controller serial number in the above example with the serial number of your *THIS* controller.

   You should expect a normal SHOW THIS response.
4. Change to the BAT subdirectory in the *scripts* directory.

31. Run the *hsg_fb1.bat* file.
32. You will see a message asking what type of failback to run. Enter **f** for a full failback.
33. You will see a confirmation message that asks you to confirm that a full failback is desired. Enter **y** for yes. If prompted, enter **v** for verbose.
34. The display indicates when mirroring is complete. At this time, the system is disaster tolerant and can operate in this mode until you choose to complete the failback process.
35. To complete the failback to the original initiator site, run the *hsg_fb2.bat* file.
36. You will see a message asking what type of failback to run. Enter **f** for a full failback.
37. You will see a confirmation message that asks you to confirm that a full failback is desired. Enter **y** for yes. If prompted, enter **v** for verbose.
38. Boot the target hosts now, to be ready for a future failover.
39. Continue with the full failback procedure at the initiator site with "Initiator Site Cleanup Procedure."

**********SANFRAN**********

Exercise 7 - Initiator Site Cleanup Procedure

1. Allow the initiator host to recognize new units. If you *have not* changed the UNIT_OFFSET of any host connections since the hosts have been booted, you do not need to reboot the initiator site hosts.
2. Open Computer Management and click Disk Management.
3. After *Disk Management* has initialized, go to the *Action Menu* and click *Rescan Disks*. All of the failed over units should appear in the right-hand pane. If Secure Path is not installed correctly, you will see each unit twice.

   If you *have* changed the UNIT_OFFSET of any host connections, you must reboot that host. You should be able to see all of the units in Disk Management.

**********SANFRAN**********

Exercise 7 - Initiator Host SQL Recovery

1. Restart the SQL Server services.
2. Open SQL Enterprise Manager. Verify that the *PseudoApplicationDB* database is attached.

   If the failover has cause the database to be suspect (error from SQL Server),

   c. Stop and restart the SQL Server service

   d. If you still have a problem, truncate the log for that database

> **!** **Important**
> In a customer environment a suspect database would require a more robust recovery method.

3. Locate *iSQLw.exe*. Double-click *iSQLw.exe*.
4. Log in using user id *admin* and no password. Use the defaults for any other parameters.
5. In iSQLw, select *File* → *Open* → *CreateOriginal_DRM.sql*.
6. Click the green arrow (run) icon in the menu bar to execute the SQL script.
7. After a few seconds, stop the script.
8. In iSQLw, select *File* → *Open* → *ShowCount.sql*.
9. Click the green arrow (run) icon in the menu bar to execute the SQL script.

   Write down the number displayed in the Result tab: .....
10. In iSQLw, select *File* → *Open* → *ShowData.sql*.
11. After verifying that the data is there, stop the query.

Unplanned Loss of Target Site Procedure

When the error mode of the remote copy set is in failsafe, and the connection to the target site is lost, host I/O is paused. This occurs because the initiator state of the remote copy set becomes inoperative while being failsafe locked.

These procedures are used to resume host I/O until the connection to the target site is re-established. The procedures are:

- Verification of Lost Connections Procedure
- Running the Resumption of Operations Batch File Procedure
- Initiator Site Cleanup Procedures
- Running the Resumption of Operations Batch File Procedure

**********SANFRAN**********

Exercise 1: Application Startup

In a business environment, one need to replicate data would be the need to continue using a database after a site failure. In this exercise, we will start a simulated database application. When the target site becomes unavailable, it will be necessary to regain operation of the database.

> **Note**
> Your instructor will point you to the files necessary to start this application data simulation if the scripts on not in *c:\scripts*.

1. Using Windows Explorer, find the executable *iSQLw.exe*. Double-click *WinSQL.exe*.
2. Log in using with user id *admin* and no password. Use the defaults for the other parameters.
3. From the same directory, select File → Open → CreateOriginal_DRM.sql.

   The SQL statement in this query creates a simulation of data entry in a database application.
4. Click the green arrow (run) icon in the menu bar to execute the SQL script.
5. Leave the iSQLw window open with the script running.
6. To simulate the loss of the target site, unplug **both** ISL fibre connections that connect the initiator site to the target site.

   The SQL script will be stopped because the storage has paused I/O activity.

**********SANFRAN**********

Exercise 2: Verification of Lost Connections Procedure

1. Verify that the connection to the target site is lost and host I/O is paused. If you are connected to the initiator site controllers when connection to the target site is lost, you will see a confirmation message on your terminal.
2. Host I/O to the remote copy sets will be paused. Verify that the initiator state of the remote copy set is inoperative, with unit failsafe locked, with the following command:

```
SHOW REMOTE_COPY_SETS FULL

        ---------------------------------------------------------------
        RCS_D1 remote copy D1 AS_SQL
        Reported LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003E
        Switches:
        OPERATION_MODE = SYNCHRONOUS
        ERROR_MODE = FAILSAFE
        FAILOVER_MODE = MANUAL
        OUTSTANDING_IOS = 20
        Initiator (SANFRAN\D1) state:
        INOPERATIVE
        Unit failsafe locked
        Target state:
        SANJOSE\D1 is COPYING 0% complete
```

**********SANFRAN**********

Exercise 3: Running the Resumption of Operations Batch File Procedure

1. Open a command prompt window on the initiator host.
2. Verify that the script server can communicate with the initiator controller via Command Scripter.

   For SCSI-3, use the command:

   ```
   cmdscript -n Z600300487 "show this"
   ```

   Note
   You would replace the controller serial number in the above example with the serial number of your *THIS* controller.

   You should expect a normal SHOW THIS response.
3. Check the error mode, initiator state, and target status of all remote copy sets with the CLI command:

   ```
   cmdscript -n Z600300487 "SHOW REMOTE_COPY_SETS FULL"
   ```

   Note
   You would replace the controller serial number in the above example with the serial number of your *THIS* controller.

7. Change to the BAT subdirectory in the CLONE_HOME directory.
8. Run the *hsg_op.bat* file.
9. You will see a message that you are performing a DRM operation to modify error mode, and asks whether normal or configured error mode is desired. Enter **n** for normal mode.
10. You will see a confirmation message that asks you to confirm that a normal error mode is desired. Enter **y** for yes. Enter **v** for verbose.
11. When an operation completion status result is displayed, verify that the script removed the targets by entering the following command:

    ```
    cmdscript -n Z600300487 "SHOW REMOTE_COPY_SETS FULL"
    ```

    Note
    You would replace the controller serial number in the above example with the serial number of your *THIS* controller.

**********SANFRAN**********

Exercise 4: Initiator Site Cleanup Procedure

1. Allow the initiator host to recognize new units. If you *have not* changed the UNIT_OFFSET of any host connections since the hosts have been booted, you do not need to reboot the initiator site hosts.
2. Open Computer Management and click Disk Management.
3. After *Disk Management* has initialized, go to the *Action Menu* and click *Rescan Disks*. All of the failed over units should appear in the right-hand pane. If Secure Path is not installed correctly, you will see each unit twice.

   If you *have* changed the UNIT_OFFSET of any host connections, you must reboot that host. You should be able to see all of the units in Disk Management.

**********SANFRAN**********

Exercise 5: Initiator Host SQL Recovery

1. Restart the SQL Server services.
2. Open SQL Enterprise Manager. Verify that the *PseudoApplicationDB* database is attached.
3. Locate *iSQLw.exe*. Double-click *iSQLw.exe*.
4. Log in using user id *admin* and no password. Use the defaults for any other parameters.
5. In iSQLw, select *File* → *Open* → *CreateOriginal_DRM.sql*.
6. Click the green arrow (run) icon in the menu bar to execute the SQL script.
7. After a few seconds, stop the script.
8. In iSQLw, select *File* → *Open* → *ShowCount.sql*.
9. Click the green arrow (run) icon in the menu bar to execute the SQL script.

   Write down the number display in the Result tab.

   .....
10. Reconnect both ISLs and allow the remote copy sets to fully normalize.
11. Type:

```
SET RCS_D1 ADD=SANJOSE\D1
SET RCS_D2 ADD=SANJOSE\D2
```

12. Allow the remote copy sets to normalize.

Planned Site Failover with Full Failback

These procedures are used to ensure the proper functioning of a planned failover and subsequent full failback for extended initiator site maintenance activities. It is expected that the duration of the event exceeds the ability of the write history log to capture all of the host I/O. Therefore, a full normalization of the remote copy sets is needed after failback. The procedures are:

- Initiator Site Preparation Procedure
- Running the Extended Planned Failover Batch File Procedure
- Target Host Setup Procedure
- Running the Full Failback Batch Files Procedure
- Initiator Site Cleanup Procedure

**********SANFRAN**********

Exercise 1: Application Startup

In a business environment, one need to replicate data would be the need to continue using a database during an extended maintenance window. In this exercise, we will run a simulated database application. We will then shutdown operation of the database at the initiator site for planned maintenance. So that business operations can continue, we will make the database available at the target site.

1. Using Windows Explorer, find the executable *iSQLw.exe*. Double-click *iSQLw.exe*.
2. Log in using with user id *admin* and no password. Use the defaults for the other parameters.
3. From the same directory, select *File* → *Open* → *CreateOriginal_DRM.sql*.
4. The SQL statement in this query creates a simulation of data entry in a database application.
5. Click the green arrow (run) icon in the menu bar to execute the SQL script.
6. Leave the iSQLw script running for a few seconds, then stop the script.
7. Locate *detachDB.bat* in the c:\scripts directory of your initiator site. Double-click *detachDB.bat*.
8. Using SQL Enterprise Manager, verify that the database has been detached. It may require that the manager is closed and re-opened to refresh the database list.
9. Shutdown the initiator host.

**********SANJOSE**********

Exercise 2: Running the Resumption of Operations Batch File Procedure

1. Open a command prompt window on the target host.
2. Verify that the script server can communicate with the target controller via Command Scripter.

   For SCSI-3, use the command:

   ```
   cmdscript -n Z600300487 "show this"
   ```

   Note
   You would replace the controller serial number in the above example with the serial number of your *THIS* controller.

   You should expect a normal SHOW THIS response.
3. Change to the BAT subdirectory in the CLONE_HOME directory.
4. Run the *hsg_fo.bat* file.

12. You will see a message asking what type of failover to run. Enter **p** for planned failover.
13. You will see a confirmation message that asks you to confirm that a planned failover is desired. Enter **y** for yes. Enter **s** for short.

**********SANJOSE**********

Exercise 3 - Target Host Setup Procedure

1. To verify that failover completed successfully, issue this CLI command:

   ```
   SHOW REMOTE_COPY_SETS FULL
   ```

   The output shows the status of remote copy sets. Be sure the units listed under Initiator State are at the target site.

2. To verify that the target hosts can connect to the LUNs, use this command:

   ```
   SHOW UNITS FULL
   ```

   In the Access field of the display, all units that are used by remote copy sets should show that the target hosts connections are enabled. This should also show the initiator controller connections.

3. Allow the target host to recognize new units. If you *have not* changed the UNIT_OFFSET of any host connections since the hosts have been booted, you do not need to reboot the target site hosts.

4. Open Computer Management and click Disk Management.

14. After *Disk Management* has initialized, go to the *Action Menu* and click *Rescan Disks*. All of the failed over units should appear in the right-hand pane. If Secure Path is not installed correctly, you will see each unit twice.

    If you *have* changed the UNIT_OFFSET of any host connections, you must reboot that host. You should be able to see all of the units in Disk Management.

**********SANJOSE**********

Exercise 4 - Target Host SQL Recovery

1. Locate *attachDB.bat* in the c:\scripts directory of your remote site. Double-click *attachDB.bat*.
2. Open SQL Enterprise Manager. Verify that the *PseudoApplicationDB* database has been attached.
3. Locate *iSQLw.exe* from your remote site. Double-click *iSQLw.exe*.
4. Log in using user id *admin* and no password. Use the defaults for any other parameters.
5. In iSQLw, select *File* → *Open* → *CreateData_DRM_Target.sql*.
6. Click the green arrow (run) icon in the menu bar to execute the SQL script.
7. After a few seconds, stop the script.
8. In iSQLw, select *File* → *Open* → *ShowCount.sql*.
9. Click the green arrow (run) icon in the menu bar to execute the SQL script.

   Write down the number displayed in the Result tab.

   .....
10. In iSQLw, select *File* → *Open* → *ShowData.sql*.
11. Maximize the iSQLw window.
12. Click the green arrow (run) icon in the menu bar to execute the SQL script.

    Can you tell where the data originated? (Hint: It's part of the record)

    .....
13. Locate *detachDB.bat* in the c:\scripts directory of your remote site. Double-click *detachDB.bat*.
14. Using SQL Enterprise Manager, verify that the database has been detached. It may require that the manager is closed and re-opened to refresh the database list.

**********SANJOSE**********

Exercise 5 - Running the Full Failback Batch Files Procedure

1. Bring the initiator host back online.
2. Open a command prompt window on the target host.
3. Verify that the script server can communicate with the target (SanFran) controller via Command Scripter.

   For SCSI-3, use the command:

   ```
   cmdscript -n Z600300487 "show this"
   ```

   Note
   You would replace the controller serial number in the above example with the serial number of your *THIS* controller.

   You should expect a normal SHOW THIS response.
4. Change to the BAT subdirectory in the CLONE_HOME directory.

15. Run the *hsg_fb1.bat* file.
16. You will see a message asking what type of failback to run. Enter **f** for a full failback.
17. You will see a confirmation message that asks you to confirm that a full failback is desired. Enter **y** for yes. If prompted, enter **v** for verbose.
18. The display indicates when mirroring is complete. At this time, the system is disaster tolerant and can operate in this mode until you choose to complete the failback process.
19. To complete the failback to the original initiator site, run the *hsg_fb2.bat* file.
20. You will see a message asking what type of failback to run. Enter **f** for a full failback.
21. You will see a confirmation message that asks you to confirm that a full failback is desired. Enter **y** for yes. If prompted, enter **v** for verbose.
22. Boot the target hosts now, to be ready for a future failover.
23. Continue with the full failback procedure at the initiator site with "Initiator Site Cleanup Procedure."

**********SANFRAN**********

Exercise 6: Initiator Site Cleanup Procedure

1. Allow the initiator host to recognize new units. If you *have not* changed the UNIT_OFFSET of any host connections since the hosts have been booted, you do not need to reboot the initiator site hosts.
2. Open Computer Management and click Disk Management.
3. After *Disk Management* has initialized, go to the *Action Menu* and click *Rescan Disks*. All of the failed over units should appear in the right-hand pane. If Secure Path is not installed correctly, you will see each unit twice.

   If you *have* changed the UNIT_OFFSET of any host connections, you must reboot that host. You should be able to see all of the units in Disk Management.

**********SANFRAN**********

Exercise 7 - Initiator Host SQL Recovery

1. Locate *attachDB.bat* in the c:\scripts directory of your initiator site. Double-click *attachDB.bat*.
2. Open SQL Enterprise Manager. Verify that the *PseudoApplicationDB* database has been attached.
3. Locate *iSQLw.exe* from your initiator site. Double-click *iSQLw.exe*.
4. Log in using user id *admin* and no password. Use the defaults for any other parameters.
5. In iSQLw, select *File* → *Open* → *CreateDRM_Original.sql*.
6. Click the green arrow (run) icon in the menu bar to execute the SQL script.
7. After a few seconds, stop the script.
8. In iSQLw, select *File* → *Open* → *ShowCount.sql*.

   Click the green arrow (run) icon in the menu bar to execute the SQL script.

   Write down the number displayed in the Result tab.

   .....
9. In iSQLw, select *File* → *Open* → *ShowData.sql*.
10. Maximize the iSQLw window.
11. Click the green arrow (run) icon in the menu bar to execute the SQL script.

    Can you tell where the data originated? (Hint: It's part of the record)

    .....

Planned Site Role Reversal

These procedures are used to implement a planned failover and subsequent simple failback for a site role reversal. The procedures are:

- Initiator Site Preparation Procedure
- Running the Role Reversal Failover Batch File Procedure
- Target Host Setup Procedure
- Running the Role Reversal Failback Batch File Procedure
- Initiator Site Cleanup Procedure

**********SANFRAN**********

Exercise 1: Application Startup

In a business environment, one need to replicate data would be the need to reverse the roles that the initiator and target subsystems use. In this exercise, we will run a simulated database application. We will then shutdown operation of the database at the initiator site for a planned role reversal. So that business operations can continue, we will make the database available at the target site, which will then be the new initiator site.

1. Using Windows Explorer, find the executable *iSQLw.exe*. Double-click *iSQLw.exe*.
2. Log in using with user id *admin* and no password. Use the defaults for the other parameters.
3. From the same directory, select *File* → *Open* → *CreateOriginal_DRM.sql*.

   The SQL statement in this query creates a simulation of data entry in a database application.

24. Click the green arrow (run) icon in the menu bar to execute the SQL script.
25. Leave the iSQLw script running for a few seconds, then stop the script.
26. Locate *detachDB.bat* in the c:\scripts directory of your initiator site. Double-click *detachDB.bat*.
27. Using SQL Enterprise Manager, verify that the database has been detached. It may require that the manager is closed and re-opened to refresh the database list.
28. Shutdown the initiator host.

**********SANJOSE**********

Exercise 2: Running the Role Reversal Failover Batch File Procedure

1. Open a command prompt window on the target host.
2. Verify that the script server can communicate with the target controller via Command Scripter.

   For SCSI-3, use the command:

   ```
   cmdscript -n Z600300487 "show this"
   ```

   Note
   You would replace the controller serial number in the above example with the serial number of your *THIS* controller.

   You should expect a normal SHOW THIS response.
3. Change to the BAT subdirectory in the CLONE_HOME directory.
4. Run the *hsg_fo.bat* file.
5. You will see a message asking what type of failover to run. Enter **r** for role reversal failover.
6. You will see a confirmation message that asks you to confirm that a planned failover is desired. Enter **y** for yes. Enter **v** for verbose.

**********SANJOSE**********

Exercise 3 - Target Host Setup Procedure

1. To verify that failover completed successfully, issue this CLI command:

   ```
   SHOW REMOTE_COPY_SETS FULL
   ```

   The output shows the status of remote copy sets. Be sure the units listed under Initiator State are at the target site.

2. To verify that the target hosts can connect to the LUNs, use this command:

   ```
   SHOW UNITS FULL
   ```

   In the Access field of the display, all units that are used by remote copy sets should show that the target hosts connections are enabled. This should also show the initiator controller connections.

3. Allow the target host to recognize new units. If you *have not* changed the UNIT_OFFSET of any host connections since the hosts have been booted, you do not need to reboot the target site hosts.

4. Open *Computer Management* and click *Disk Management*.

5. After *Disk Management* has initialized, go to the *Action Menu* and click *Rescan Disks*. All of the failed over units should appear in the right-hand pane. If Secure Path is not installed correctly, you will see each unit twice.

   If you *have* changed the UNIT_OFFSET of any host connections, you must reboot that host. You should be able to see all of the units in Disk Management.

**********SANJOSE**********

Exercise 4 - Target Host SQL Recovery

1. Locate *attachDB.bat* in the c:\scripts directory of your remote site. Double-click *attachDB.bat*.
2. Open SQL Enterprise Manager. Verify that the *PseudoApplicationDB* database has been attached.
3. Locate *iSQLw.exe* from your remote site. Double-click *iSQLw.exe*.
4. Log in using user id *admin* and no password. Use the defaults for any other parameters.
5. In iSQLw, select *File* → *Open* → *CreateData_DRM_Target.sql*.
6. Click the green arrow (run) icon in the menu bar to execute the SQL script.
7. After a few seconds, stop the script.
8. In iSQLw, select *File* → *Open* → *ShowCount.sql*.
9. Click the green arrow (run) icon in the menu bar to execute the SQL script.

   Write down the number displayed in the Result tab.

   .....
10. In iSQLw, select *File* → *Open* → *ShowData.sql*.
11. Maximize the iSQLw window.
12. Click the green arrow (run) icon in the menu bar to execute the SQL script.

    Can you tell where the data originated? (Hint: It's part of the record)

    .....

12. Locate *detachDB.bat* in the c:\scripts directory of your remote site. Double-click *detachDB.bat*.
14. Using SQL Enterprise Manager, verify that the database has been detached. It may require that the manager is closed and re-opened to refresh the database list.

**********SANJOSE**********

Exercise 5 - Running the Full Failback Batch Files Procedure

1. Bring the initiator host back online.
2. Open a command prompt window on the target host.
3. Verify that the script server can communicate with the target controller via Command Scripter.

   For SCSI-3, use the command:

   ```
   cmdscript -n Z600300487 "show this"
   ```

   Note

   You would replace the controller serial number in the above example with the serial number of your *THIS* controller.

   You should expect a normal SHOW THIS response.

29. Change to the BAT subdirectory in the CLONE_HOME directory.
30. Run the *hsg_fb1.bat* file.
31. You will see a message asking what type of failback to run. Enter **r** for a role reversal failback.
32. You will see a confirmation message that asks you to confirm that a role reversal failback is desired. Enter **y** for yes. If prompted, enter **v** for verbose.
33. The display indicates when mirroring is complete.
34. Boot the target hosts now, to be ready for a future failover.
35. Continue with the full failback procedure at the initiator site with "Initiator Site Cleanup Procedure."

**********SANFRAN**********

Exercise 6: Initiator Site Cleanup Procedure

1. Allow the initiator host to recognize new units. If you *have not* changed the UNIT_OFFSET of any host connections since the hosts have been booted, you do not need to reboot the initiator site hosts.
2. Open Computer Management and click *Disk Management*.
3. After Disk Management has initialized, go to the Action Menu and click *Rescan Disks*. All of the failed over units should appear in the right-hand pane. If Secure Path is not installed correctly, you will see each unit twice.

   If you **have** changed the UNIT_OFFSET of any host connections, you must reboot that host. You should be able to see all of the units in Disk Management.

**********SANFRAN**********

Exercise 7 - Initiator Host SQL Recovery

1. Locate *attachDB.bat* in the c:\scripts directory of your initiator site. Double-click *attachDB.bat*.
2. Open SQL Enterprise Manager. Verify that the *PseudoApplicationDB* database has been attached.
3. Locate *iSQLw.exe* from your initiator site. Double-click *iSQLw.exe*.
4. Log in using user id *admin* and no password. Use the defaults for any other parameters.
5. In iSQLw, select *File* → *Open* → *CreateDRM_Original.sql*.
6. Click the green arrow (run) icon in the menu bar to execute the SQL script.
7. After a few seconds, stop the script.
8. In iSQLw, select *File* → *Open* → *ShowCount.sql*.
9. Click the green arrow (run) icon in the menu bar to execute the SQL script.

   Write down the number displayed in the Result tab.

   .....
10. In iSQLw, select *File* → *Open* → *ShowData.sql*.
11. Maximize the iSQLw window.
12. Click the green arrow (run) icon in the menu bar to execute the SQL script.

    Can you tell where the data originated? (Hint: It's part of the record)

    .....

DRM Scripting Lab is now complete.

Please let your instructor know that you are finished.

addendum 1

hp StorageWorks secure path 3.1 for Windows lab

Objective

Your customer, Widget Inc., is continuously upgrading their network infrastructure to ensure that they are providing the highest levels of fault tolerance available to them. As their data becomes increasingly critical, they would like to implement higher levels of fault tolerance. Knowing that hardware failures can mean costly downtime, they want to implement multipathing software.

After completing this lab, you should be able to understand the installation and operation of HP StorageWorks Secure Path software.

Prerequisites

- One HSG80-based storage subsystem
- Two HSG80 controllers configured for multibus failover mode
- At least four disk drives installed in the drive cabinet
- At least two LUNs (D1 and D2) created in advance.
- One host running Windows 2000 Advanced Server (SP2 or later) with two 64-bit 33MHz HP (Emulex) Fibre Channel host bus adapters (HBAs)—Do not connect the HBAs to the switch (or hub) until you are instructed to do so.
  - Firmware version for the HBA: SF3.81 a1
  - Device driver: 5.4.41a7 or 5.4.52a8
- ACS version 8.6-1P or greater
- One client station running Windows 2000 (can use server)
- Six fiber cables
- Two Fibre Channel switches (8- or 16-port models)

Your instructor will provide you with the following:

- Location of Secure Path software. Write this location in the space provided below:

  .....

- Client and server can communicate via TCP/IP on the classroom LAN. Record the IP addresses of your client and server in the space provided below:

  .....

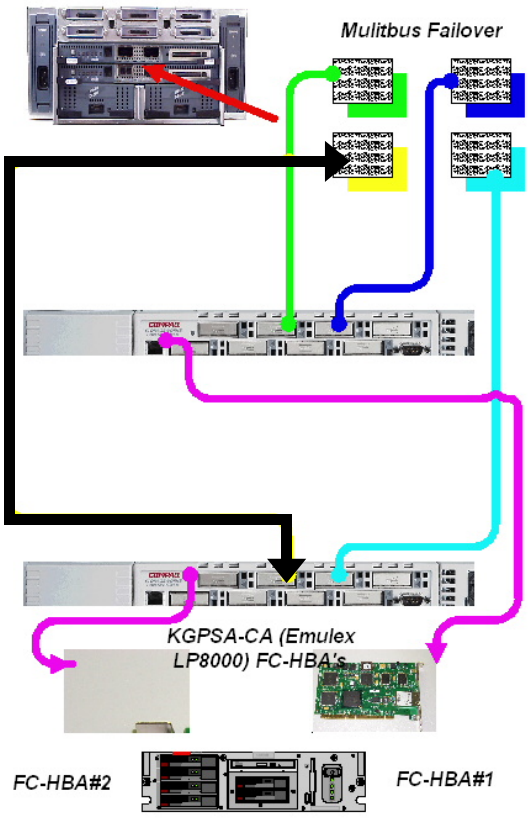
Checklist

As you complete each lab exercise, have your instructor verify that you have performed it successfully. Then check off the following list:

- ☐ Able to successfully install Secure Path as demonstrated by the successful failover of a degraded path.
- ☐ Able to manage a Secure Path profile by configuring the client list, assigning access rights, and running the Secure Path Manager interface.

Hardware Configuration and Physical Connections

Configure your lab station as shown in the diagram below.



Cabling Secure Path for DRM

Verify the following:

> **Note**
> Do not attach the fiber cables to from the host to the switch until you are instructed to do so.

- The ACS version of the controller is 8.6-1P.
- An 8- or 16-port SAN switch
- A maintenance (serial) cable connects your client station (or server) to the top HSG80 array controller. You can communicate to the subsystem using command line interface (CLI) or StorageWorks Command Console (SWCC).
- A HBA device and class drivers are loaded and are functioning properly.
- SAN switch software, ACS8.6 for multibus failover installed on the server system.

> **! Important**
> HSZdisk will not start on the server until Secure Path is installed.

> **Note**
> To successfully complete this lab exercise, ensure that you have at least two LUNs configured in your subsystem.

- Using the CLI (or SWCC) interface ensure that your controllers are in multibus failover mode and working properly.
- After connecting the first HBA to the host verify that:
  - You do not have any partitioned LUNs created behind your controllers. (Secure Path does **not** support partitioning of LUNs.)
  - None of your Windows 2000 volume sets use software RAID or extended volumes (for example, you cannot span more than one physical disk).
  - The server has the TCP/IP protocol installed (the client and agent communicate through sockets).

Setting Your HSG80-based Storage System

Important
If your controllers are already in multibus failover mode, skip the first step.

1. Initiate a CLI session from your server system to your HSG80.

   a. `Type SET NOFAILOVER`

      Take the controllers out of transparent failover mode. The other controller will shut down. Restart it by depressing its OCP Reset button, and wait a couple minutes for it to come back up.

   b. `SET MULTIBUS COPY = THIS`

      Set the controllers in multiple-bus failover mode.

      Note
      If this step is executed, both controllers will restart.

   c. `SHO THIS`

      Verify that this controller is in multiple-bus failover mode.

2. Verify that the Port-1-Topology and Port-2-Topology are set to fabric.

   If not type:

   ```
   SET THIS PORT_1_TOPOLOGY=FABRIC
   SET THIS PORT_2_TOPOLOGY=FABRIC
   ```

   Then type:

   ```
   SHO OTHER
   ```

3. Verify that the other controller is in multiple-bus failover mode.
4. Verify that the port-1-topology and port-2-topology are set to fabric.

   If not type:

   ```
   SET OTH PORT_1_TOPOLOGY=FABRIC
   SET OTH PORT_2_TOPOLOGY=FABRIC
   ```

Assigning Units to Controllers

You should assign storage units to one of the two controllers to specify which controller will be used to access the unit during server boot time. That is, you determine which controller will be doing the work for which of the units. In effect, this procedure specifies the path (controller, switch, and host adapter) on which the I/Os will travel.

You have the option of moving units around the two paths from within the Secure Path Manager GUI. For now, take the recommended action of splitting storage containers evenly between the two paths.

Type:

```
SHOW UNITS
SET D1 PREF = THIS
SET D2 PREF = OTHER
```

Note

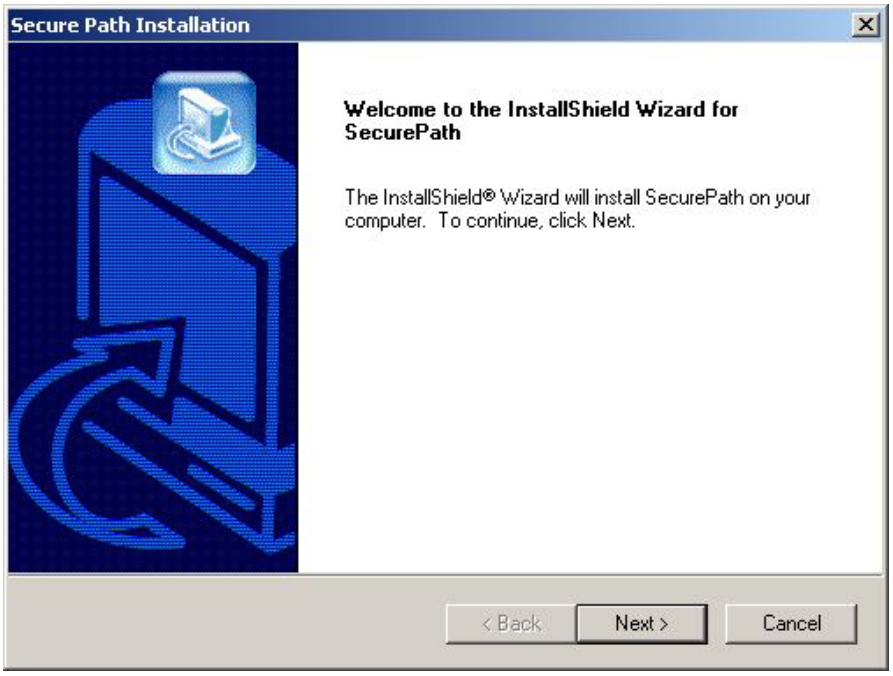
When a unit is created, it is initially set to `NO_PREFERRED_PATH`. In this case, you are letting the operating system dictate which path to choose. Because unpredictable load balancing would occur, you would **never** select this option.

Installing the Secure Path Driver and Agent

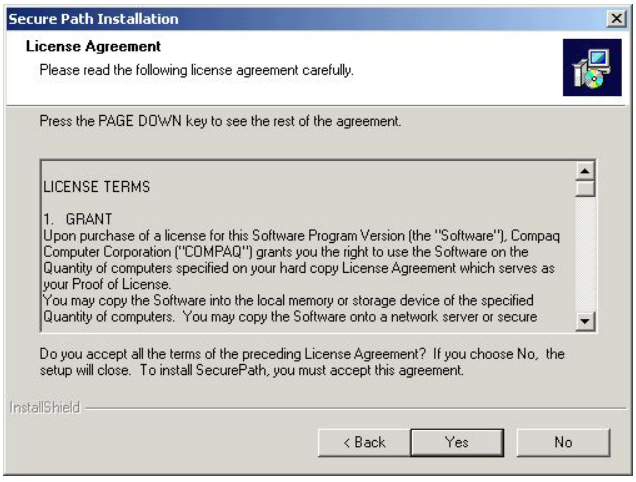
Secure Path for Windows 2000 consists of a kernel mode filter driver (RaiDisk.sys) that is responsible for directing I/O to the desired path, and for changing paths whenever the driver detects a failure in a redundant path.

Secure Path is managed by a client/server application that requires that TCP/IP be installed both on the Windows 2000 server and on the management station on which the Secure Path Manager GUI is installed. The GUI can be installed on the same server as the agent, or it can be run remotely through TCP/IP.

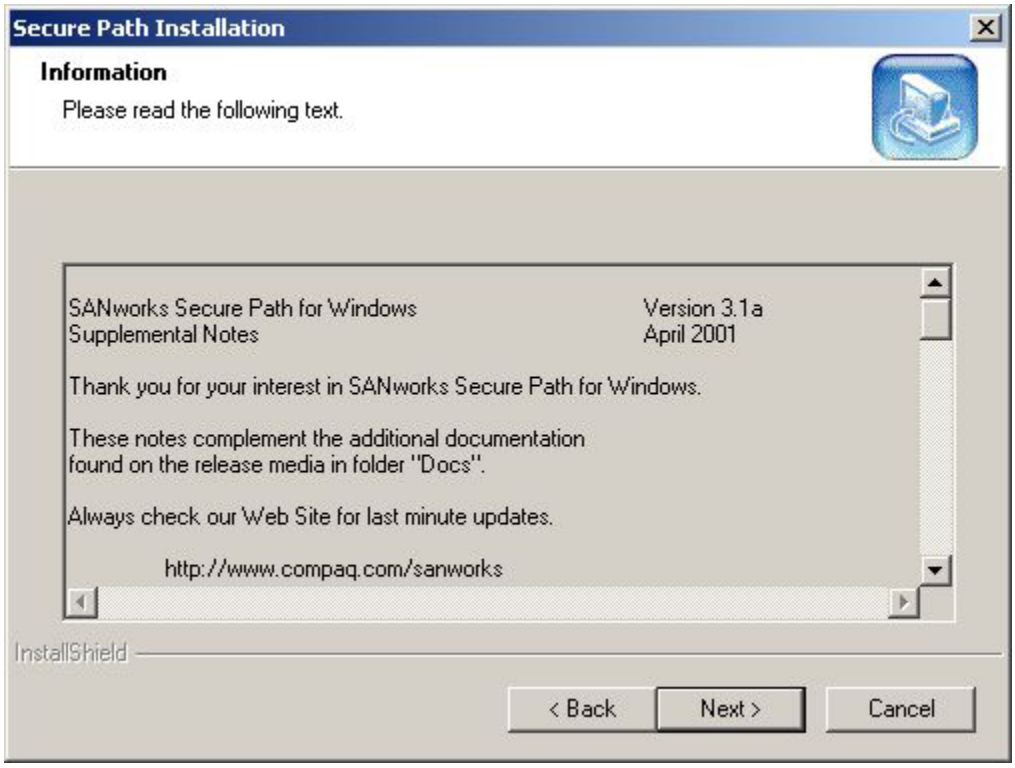
1. Locate the Secure Path installation files as directed by your instructor. Double-click *setup.exe*.



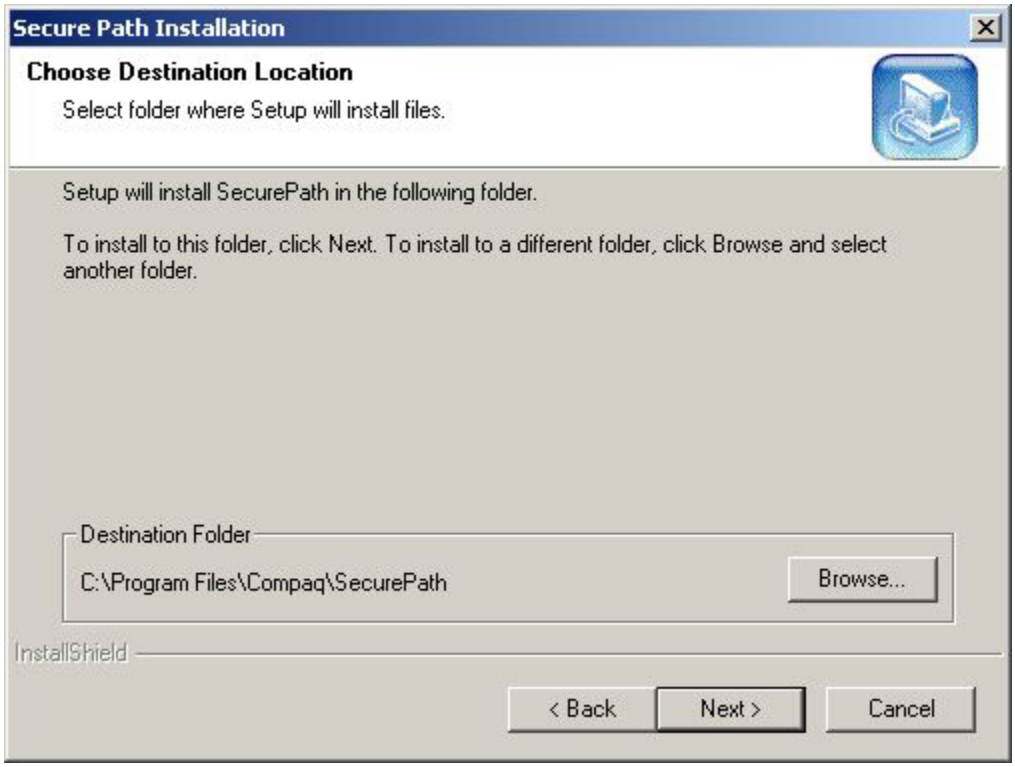
5. The Secure Path splash screen displays. Click *Next*.



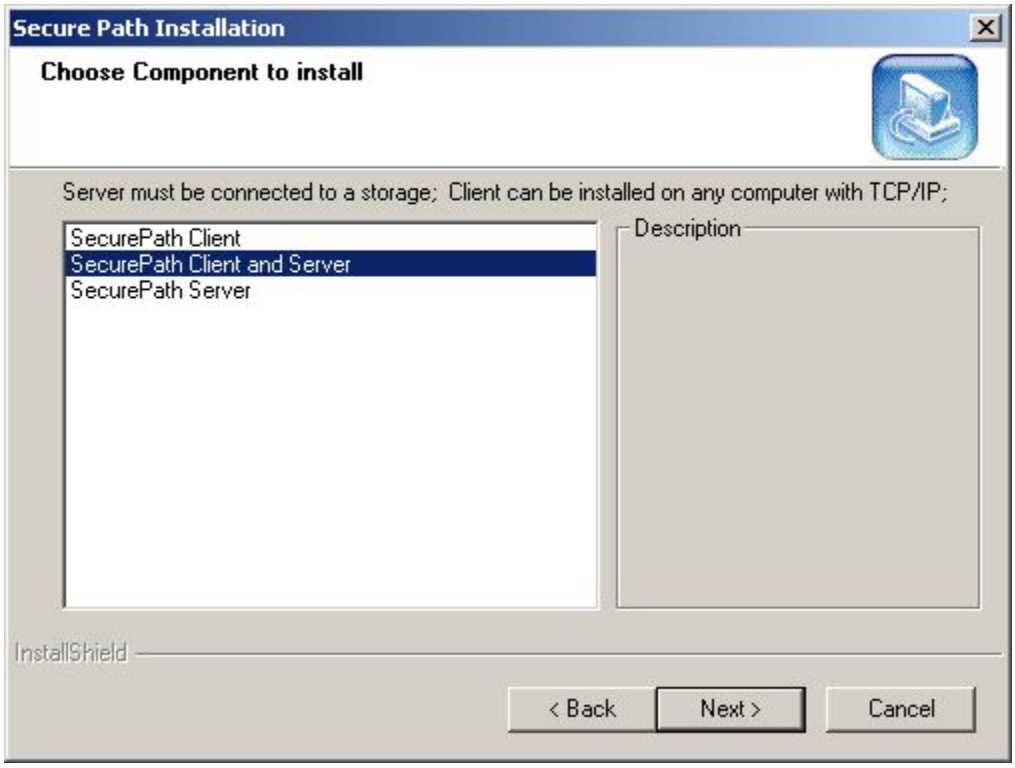
6. The Secure Path license agreement displays. Click *Yes* to agree to the terms and proceed with the installation.



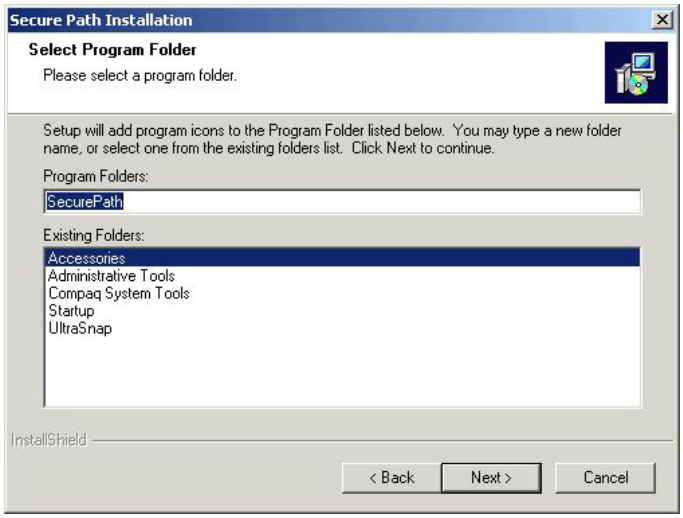
7. The next dialog box displays Secure Path release information. Scroll down the list to examine this text. When you have finished, click *Next*.



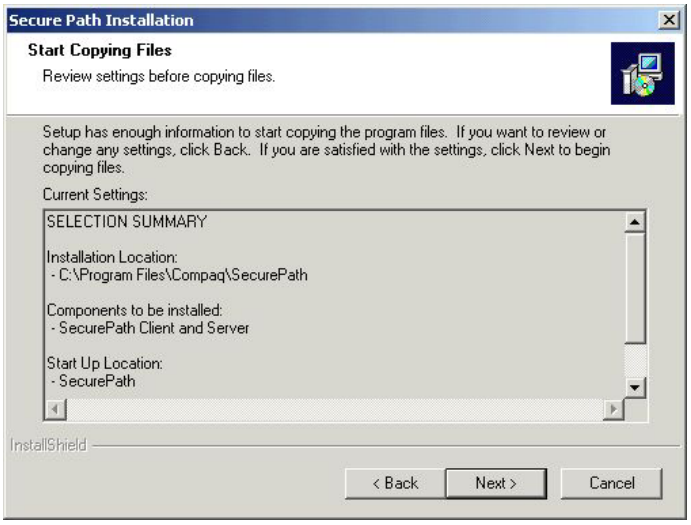
8. The next screen prompts you for the Secure Path installation directory. Accept the default and click *Next*.



9. You have the choice of loading the server (installing Secure Path drivers and agent), the client (the GUI), or both. For this lab, install both the client and the server. Select *Secure Path Client and Server,* then click *Next* to continue.

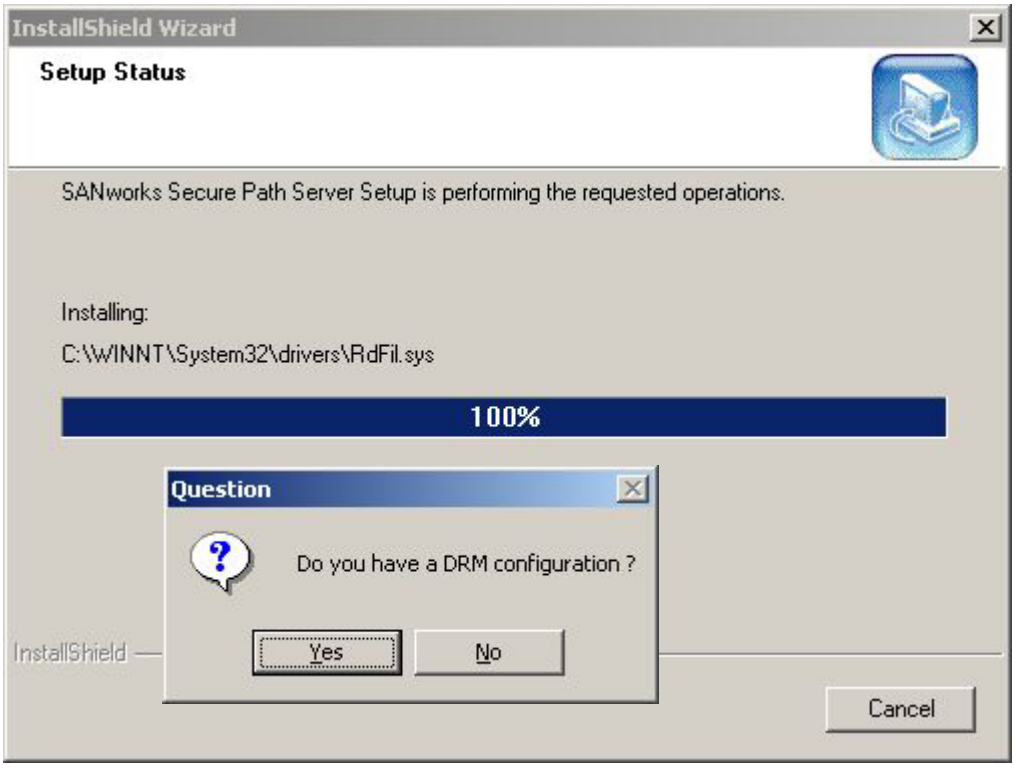


10. Accept the default installation folder and click *Next* to continue.

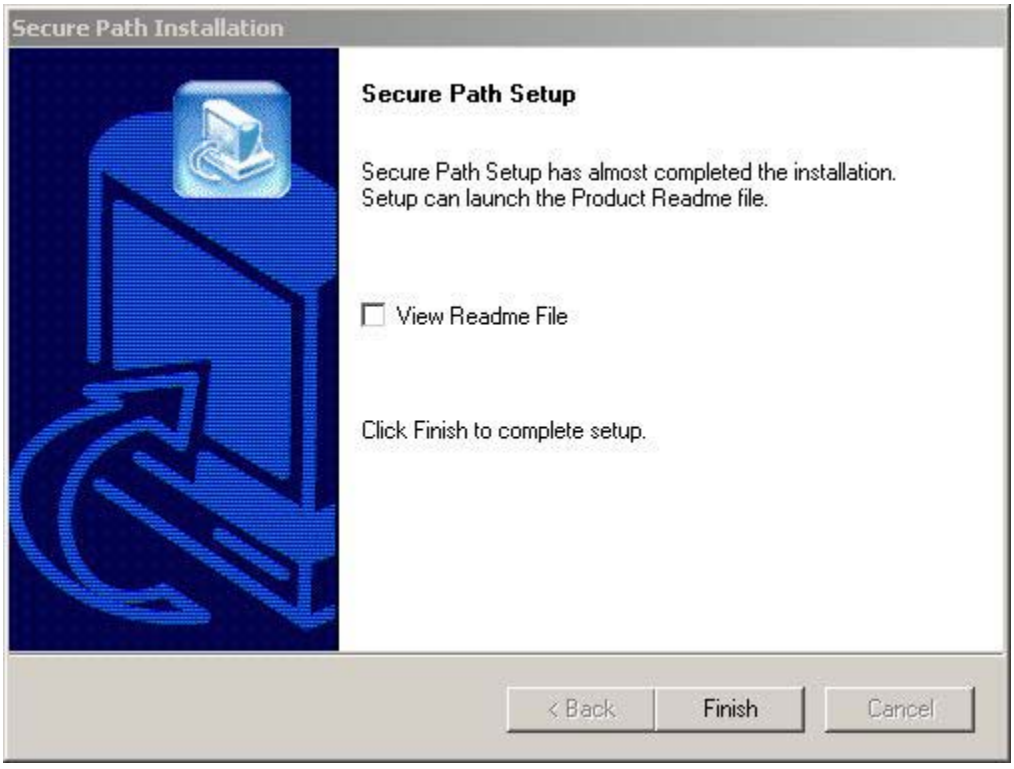


11. The next screen informs you that the setup routine is ready to begin copying the Secure Path files to your system. It also provides an opportunity to verify the installation parameters that you have already entered. Verify that the settings are correct.
12. Click *Back* if you need to make modifications, or click *Next* if the current settings are correct.

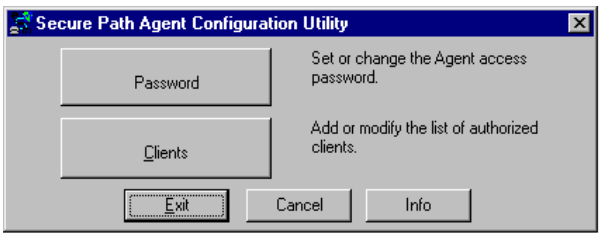
> **! Important**
> Select *No* if prompted to overwrite your current HszDisk or HBA drivers with older versions.



13. Click *Yes* to the question, "Do you have a DRM configuration?"



14. Click *Finish*.

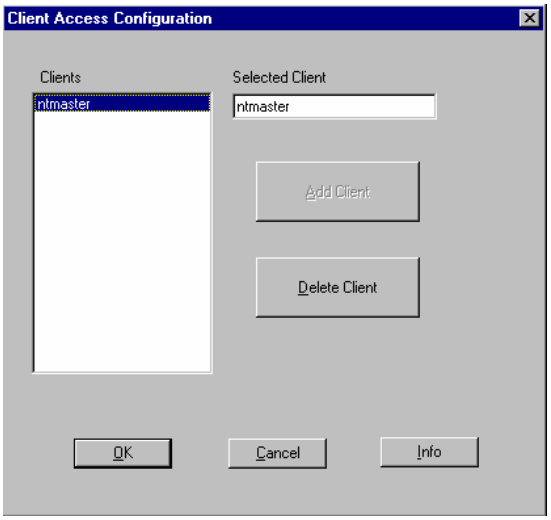


15. The Secure Path Agent Configuration Utility is similar to the utility used to configure the SWCC HS Agent.

    a. Click *Password*. Enter and confirm *12345* as your password. You will be asked for this password when you launch the Secure Path Manager later in this lab.

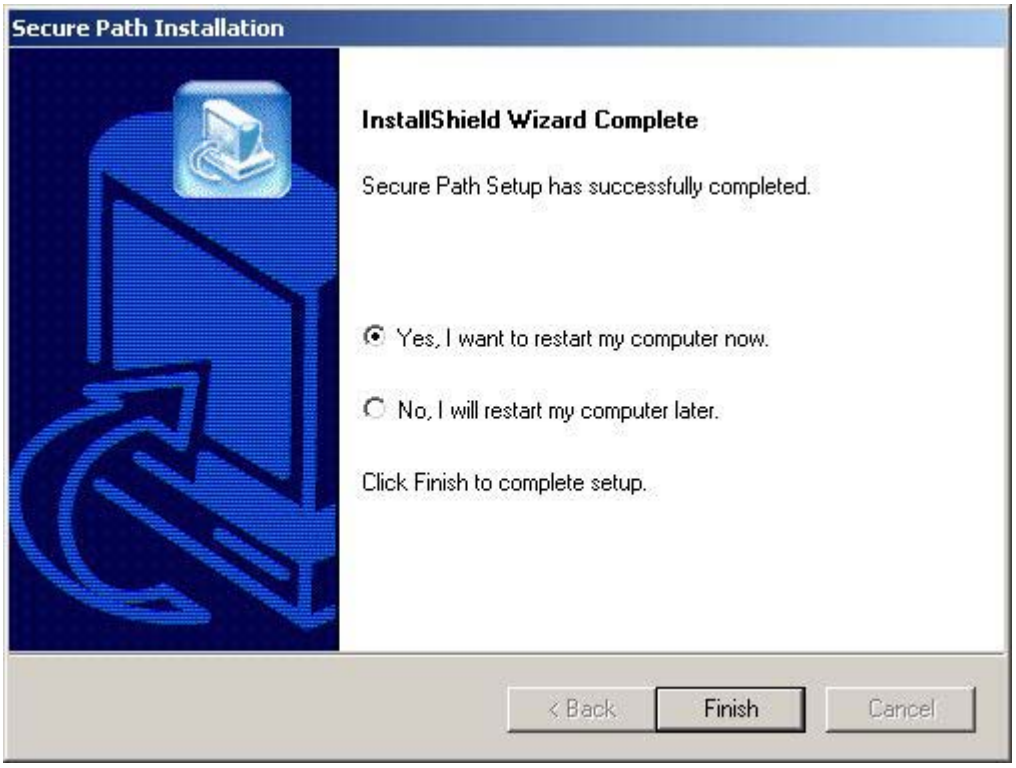
    b. Click *Clients* to configure the list of clients that will be able to manage this instance of Secure Path.

       The Clients dialog box displays.



    c. Click *OK*. You will return to the dialog box with the *Password* and *Clients* buttons. Click *Exit* to continue.

16. Click *Finish*.

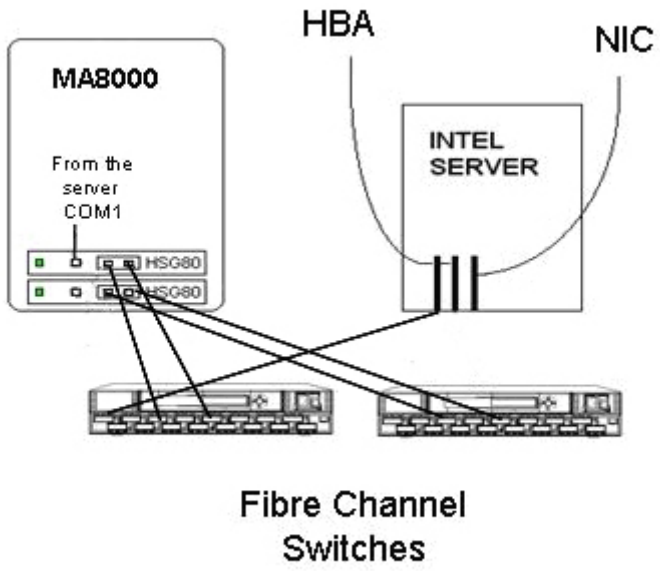


17. You will be prompted to restart your computer. Select *Yes, I want to restart my computer now* and click *Finish*.
18. After your system restarts, ensure that the *Compaq HS service* has started properly. Select *My Computer* → *Manage* → *Services and Applications* → *Services*.

Connecting the HBAs

Connecting the First HBA

1. Shut down your Windows Server. Connect the HBA to the Fibre Channel Switch as the diagram below shows:

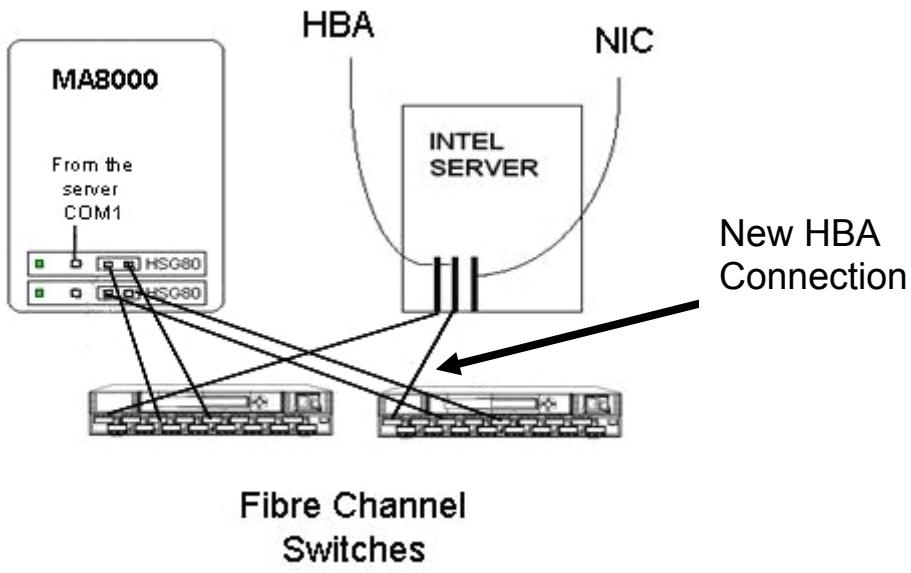


> **Important**
> Do not connect the second HBA to the switch at this time.

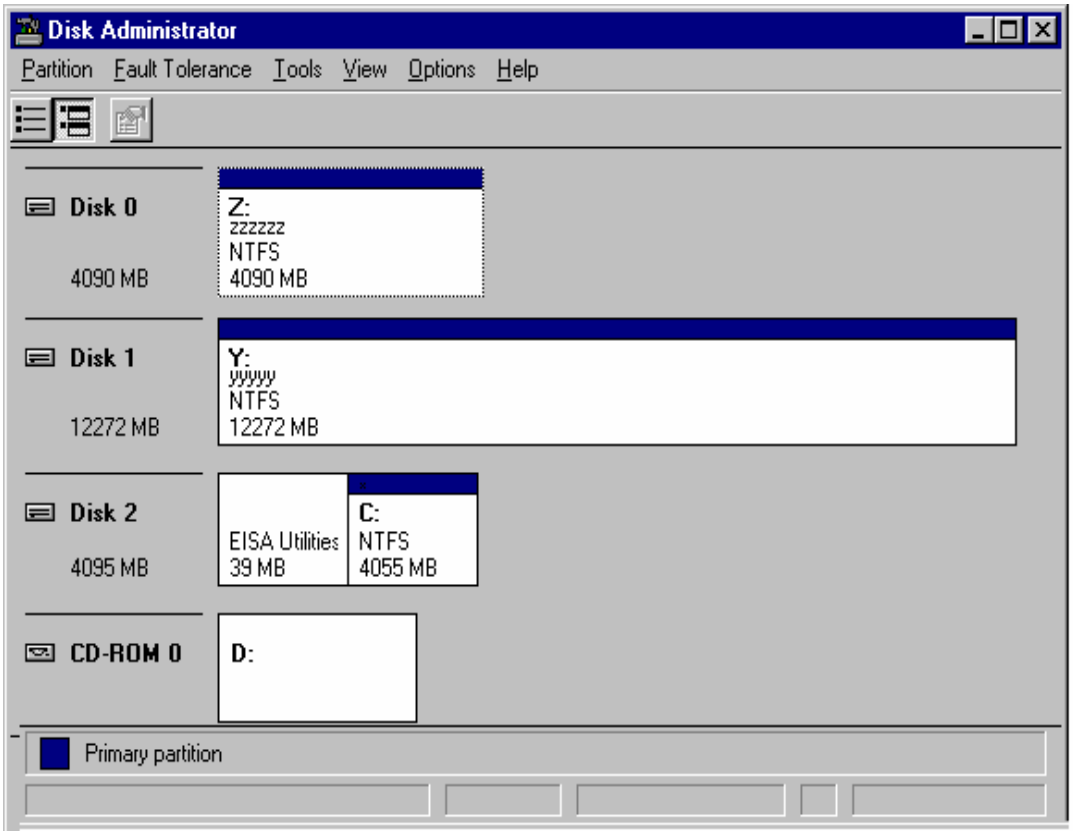
19. Power on the server.
20. Run Disk Management and write signatures to the new drives. Assign fixed drive letters to the two new drives (Y: and Z:).
21. Ensure that each unit configured by the controllers is visible to the host.
22. Format the disks using *Quick Format*. Assign the letters *Y*: to one and *Z:* to the other.

Connecting the Second HBA

1. Shut down your Windows Server. Connect the second HBA to the Fibre Channel switch as shown in the following diagram:



2. Power on the server.

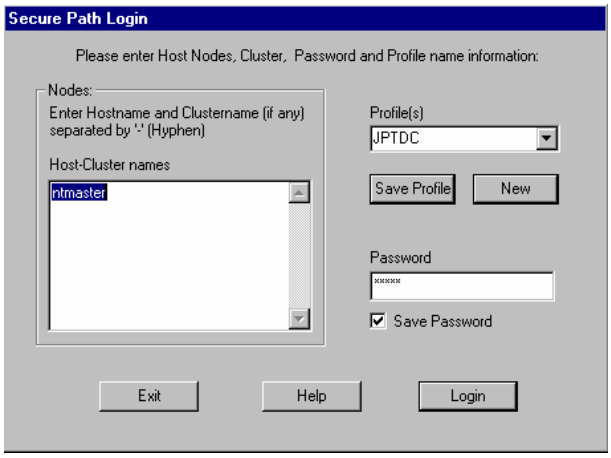


3. Select *My Computer* → *Manage* → *Disk Management*. Ensure that each unit configured by the controllers has only one disk number listed. If the installation was unsuccessful, you would see two instances of each unit, as shown above.

Using Secure Path Manager

Logging On to the Secure Path Server

1. Open *Start* → *Programs* → *SecurePath* → *SPM*. The Secure Path Login window displays.



Because this is the first time the Secure Path Manager is being run, you must type in the name of the Secure Path server, name the profile for this server, and specify a password to allow access to the Secure Path server. (12345)

2. Enter the following values.

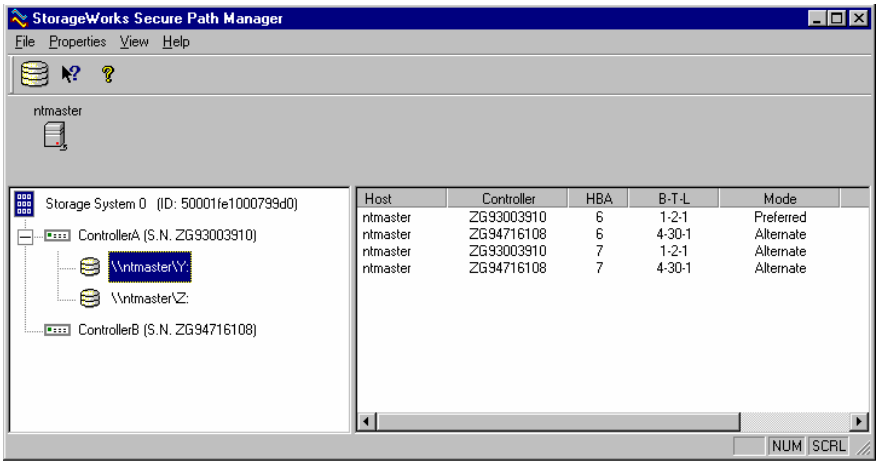
Field	Value
Host-Cluster names	Your server name
Profile(s)	Profile1
Password	12345

> **!** **Important**
> The password and client list for the Secure Path agent can be modified by selecting *Start* → *Programs* → *SecurePath* → *SecurePathCfg*.

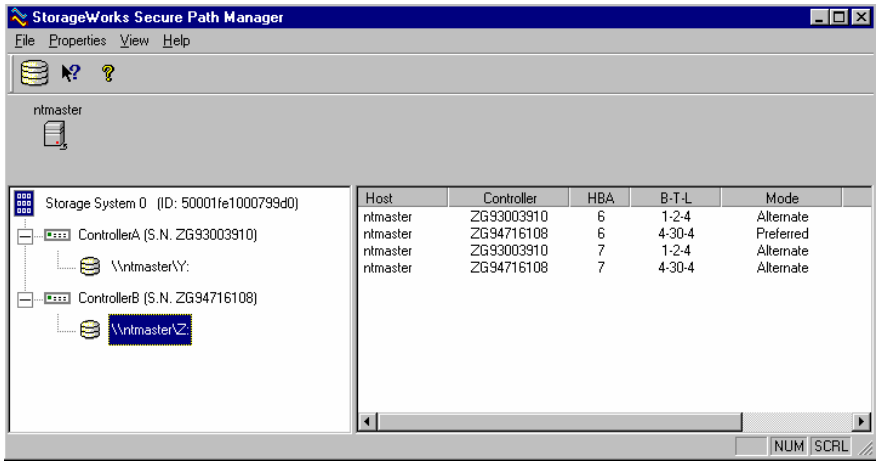
3. Click *Save Profile*.
4. Click *Login* to log in to the GUI.

Secure Path Manager displays both paths to your storage subsystem. The top path is Controller A and the bottom path is Controller B.

Information regarding each disk device displays in the content pane on the right hand side of the screen.



5. Using your mouse, click-and-hold on disk Z and drag it to the other controller.



Note

Dragging disk devices between the two paths is the method used to load balance each controller path. You must change the associated PREFERRED_PATH on the HSG80 controller to make this change permanent (for example, SET D1 PREF = OTHER). Otherwise, the next time the Windows server is restarted, the original PREFERRED_PATH unit setting will take precedence and place your disk back in its original path.

6. Select *My Computer* → *Manage* → *Disk Management*. Delete the partitions for both disks.
7. Using the serial connection and CLI, delete the LUNs and mirrorsets from your storage system.

This completes this lab exercise.

Please continue with Lab 4 — DRM Installation.