COMPAQ
STORAGEWORKS

StorageWorks Secure Path for Windows NT

A High Availability MultiPath Solution

Installation Guide

EK–WNTMP–MH. B01

Compaq Computer Corporation

Contents

2 Pre-Installation Steps

3 Installing Secure Path Software

4 Installing Secure Path Hardware

5 Using Secure Path Manager

Appendix A

Figures

Tables

Revision Record

This Revision Record provides a concise publication history of this manual. It lists the manual revision levels, release dates, and reasons for the revisions.

The following revision history lists all revisions of this publication and their effective dates. The publication part number is included in the Revision Level column, with the last entry denoting the latest revision.

Revision Level	Date	Summary of Changes
EK–WNTMP–MH. A01	June 1998	Original release. Single Host – SCSI RA7000 / ESA10000
EK–WNTMP–MH. A02	November 1998	Second release. Add Fibre Channel RA8000 / ESA12000 and Support for Microsoft Cluster Server.

About This Guide

This section defines the scope, structure and conventions of this guide. It identifies associated reference documentation, and the StorageWorks sales, service, and technical support contacts worldwide.

Audience

This guide is intended for administrators and system integrators of Intel or Alpha based host servers and StorageWorks RAID storage solutions. Setting up a Secure Path environment requires a general understanding of server networks, RAID storage concepts and device drivers, Windows NT software, SCSI and/or Fibre Channel hardware configurations. Or, contact your service representative for installation assistance.

Document Structure

This guide contains the following chapters:

Getting Started

This section provides two ways to install and configure Secure Path for Windows NT. Experienced system integrators and administrators may want to use the simplified installation instructions that are included in this chapter to quickly establish a Secure Path environment. Others may want to use the road map at the end of this chapter to read comprehensive installation instructions that serve as the master procedural reference guide for establishing a Secure Path environment.

Chapter 1: Pre-Installation Steps

This chapter addresses the preparation needed before installing and configuring the Secure Path components.

Chapter 2: Theory of Operation

This chapter offers an overview of Secure Path for Windows NT, and explains the operation of Secure Path in a No Single Point of Failure configuration.

Chapter 3: Installing Secure Path Software

This chapter describes the software configuration procedures required to establish a Secure Path storage environment. It includes the procedures to set the

two StorageWorks RAID controllers for multibus mode operation, prefer storagesets between the controllers, and install the StorageWorks Secure Path software on the host servers and client.

Chapter 4: Installing Secure Path Hardware

This chapter provides the procedures for preparing the host bus adapters, and interconnecting Secure Path hardware components.

Chapter 5: Using Secure Path Manager

This chapter describes features of the Secure Path Manger. The Secure Path storage environment can be monitored and managed using the Secure Path Manager. Secure Path Manager provides graphic representation of bus path vitality status, disk I/O path assignments, automatic path failover, and (manual) path failback functionality.

Appendix A: De-Installing Secure Path Software

The procedure for removing Secure Path software from your system is provided in this appendix.

Conventions

In this guide, references to RAID, RAID subsystem, *StorageWorks RAID Array, HSZ70, HSG80, controller, or subsystem* pertain to either of the following:

- UltraSCSI Raid Array 7000 or Enterprise Storage Array (ESA) 10000
- Fibre Channel Raid Array 8000 or Enterprise Storage Array (ESA) 12000

This guide uses the following documentation conventions:

Table 1 Style Conventions

Style	Meaning
boldface monospace type	To be input by the user.
italic type	For emphasis, manual titles, utilities, menus, screens, and filenames.
plain monospace type	Screen text.
HS*** >	RAID controller prompt

Getting Help

If you have a problem and have exhausted the information in this guide, you can get further information and other help in the following locations.

Compaq Web Site

The Compaq Web Site has information on this product as well as the latest drivers and Flash ROM images. You can access the Compaq Web Site by logging on to the Internet at :

http://www.compaq.com

Telephone Numbers

For the name of your nearest Compaq Authorized Reseller:

In the United States, call 1-800-345-1518
In Canada, call 1-800-263-5868
For Compaq technical support:
In the United States and Canada, call 1-800-386-2172

Getting Started

This section provides two ways to install and configure Secure Path for Windows NT. Experienced system integrators and administrators may want to use the simplified installation instructions that are included in this chapter to quickly establish a Secure Path environment. Others may want to use the road map at the end of this chapter to read comprehensive installation instructions that serve as the master procedural reference guide for establishing a Secure Path environment.. This roadmap presides over all other documentation supplied with your equipment, and refers to those resources, as more technical depth is required.

Quick Setup Guide

Note: You must have completed installation of a SCSI RAID Array 7000 or a Fibre Channel RAID Array 8000 in a Windows NT single server or cluster environment with a single I/O path, and it must be functioning properly. You must have established a serial line connection to the RAID Array.

Do not proceed until the single path installation is functioning properly.

Do not install Secure Path for Windows in an Alpha server which has FX!32 installed.

Use the appropriate Quick Setup Guide depending on the type of your RAID subsystem and the desired configuration.

- If you own a SCSI RAID Array 7000 or an ESA 10000 and one Windows NT server, please turn to page xv
- If you own a SCSI RAID Array 7000 or an ESA 10000 and a Windows NT Cluster with SCSI Y-cables, please turn to page xix
- If you own a SCSI RAID Array 7000 or an ESA 10000 and a Windows NT Cluster with SCSI hubs, please turn to page xxiii
- If you own a Fibre Channel RAID Array 8000 or an ESA 12000 and one Windows NT server, please turn to page xxvii
- If you own a Fibre Channel RAID Array 8000 or an ESA 12000 and a Windows NT Cluster, please turn to page xxxi.

Quick Setup Guide for

SCSI RAID Array 7000 or ESA 10000 and one Windows NT server

Note: Do not install Secure Path for Windows in an Alpha server which has FX!32 installed.

1. Inventory additional components needed

Qty	Part Number	Description
1	QB-669AA-SA	Secure path for Windows (version 1 or higher)
1	AHA2944UW	UltraSCSI Host Bus Adapter
1	SWXKT-FA	RAID SCSI Connection Kit

2. Examine present configuration

Action	✔
Single path configuration functions properly – check event log	
Serial line connection available to the controller	
StorageSets and NT volumes defined – not hardware partitioned	
Windows NT system disk not part of RAID subsystem	
TCP/IP protocol installed on Windows NT server	
[Alpha servers] FX!32 not installed	

3. Install Secure Path software

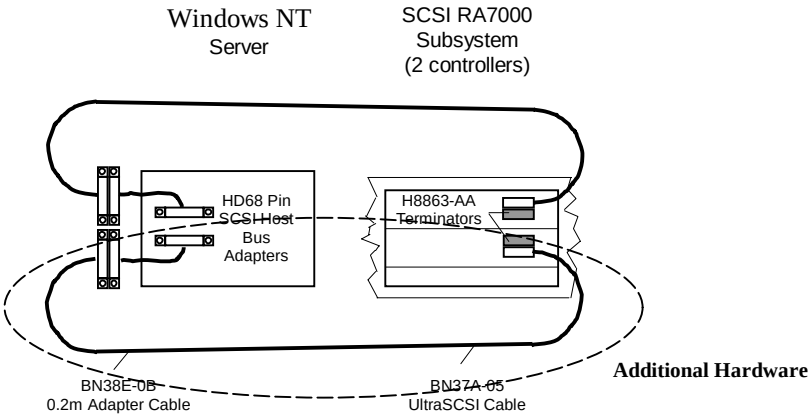
From the Secure Path CDROM, launch \SPINSTAL\SETUP.EXE, and follow directions. Setup will shutdown the server. **Do not restart the server until you have completed preparing the RAID subsystem.**

4. Prepare the RAID subsystem

After the server has shutdown, perform the following actions:

Action	**Serial Line (CLI) steps**	✔
Set the controllers to multibus failover mode	HS***> **set nofailover** *The "other" controller will shutdown and must be manually restarted by momentarily depressing the reset button on the controller's front panel.* HS***> **set multibus copy=this** *The controllers will restart in multibus mode*	
Verify that the controller mode was changed to multibus failover.	HS***> **show this** HS***> **show other**	
Prefer each storage unit to "this" or the "other" controller.	HS***> **show units** HS***> **set** *(unit#)* **preferred=this** - or - HS***> **set** *(unit#)* **preferred=other**	

5. Install additional hardware



Adaptec AHA 2944UW Settings	✔
Internal termination enabled	
Host adapter BIOS disabled	
SCSI bus reset disabled	

6. Confirm installation

Action	✔
Reboot the server	
Check event log for proper SCSI operation	
Launch Secure Path Manager	

Quick Setup Guide for

SCSI RAID Array 7000 or ESA 10000 and a Windows NT Cluster with SCSI Y-cables

Note: Do not install Secure Path for Windows in an Alpha server which has FX!32 installed.

1. Inventory additional components needed

Qty	Part Number	Description
1	QB-669AA-SA	Secure path for Windows (version 2 or higher)
2	AHA2944UW	UltraSCSI Host Bus Adapter
1	SWXKT-DF	UltraSCSI Cluster RAID Connection Kit

2. Examine present configuration

Action	✔
Single path configuration functions properly – check event log on both servers	
Serial line connection available to the controller	
StorageSets and NT volumes defined – not hardware partitioned	
Windows NT system disk not part of RAID subsystem	
TCP/IP protocol installed on both Windows NT servers	
[Alpha servers] FX!32 not installed on either server	

3. Install Secure Path software

From the Secure Path CDROM, launch \SPINSTAL\SETUP.EXE on each server, and follow directions. Setup will shutdown the server. **Do not restart the server until you have completed preparing the RAID subsystem.**

4. Prepare the RAID subsystem

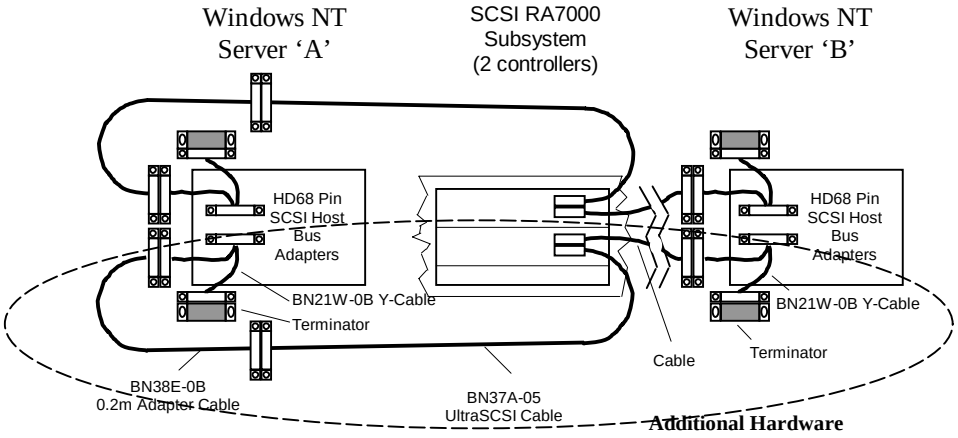
After the server has shutdown, perform the following actions:

Action	**Serial Line (CLI) steps**	✔
Set the controllers to multibus failover mode	HS***> **set nofailover** *The "other" controller will shutdown and must be manually restarted by momentarily depressing the reset button on the controller's front panel.* HS***> **set multibus copy=this** *The controllers will restart in multibus mode*	
Verify that the controller mode was changed to multibus failover.	HS***> **show this** HS***> **show other**	
Prefer each storage unit to "this" or the "other" controller.	HS***> **show units** HS***> **set** *(unit#)* **preferred=this** - or - HS***> **set** *(unit#)* **preferred=other**	

5. Install additional hardware

Adaptec AHA 2944UW Settings	✔
Internal termination **disabled**	
Host adapter BIOS **disabled**	
SCSI bus reset **disabled**	
Set unique SCSI Ids for each new adapter	

NOTE: You must assure that the connection between host adapters on both servers is consistent. Use the PCI slot numbering on your servers as a guide. The adapters on each server that connect to one controller should be in the same PCI slot in each server. If it is not possible to install the adapters in the same slot in each server, you must install them in sequence. For example, the first adapters installed in each server must connect to the same controller.



6. Confirm installation

Action	✔
Reboot the servers	
Check event log for proper SCSI operation	
Launch Secure Path Manager	

Quick Setup Guide for

SCSI RAID Array 7000 or ESA 10000 and a Windows NT Cluster with SCSI Hubs

Note: Do not install Secure Path for Windows in an Alpha server which has FX!32 installed.

1. Inventory additional components needed

Qty	Part Number	Description
1	QB-669AA-SA	Secure path for Windows (version 2 or higher)
2	AHA2944UW	UltraSCSI Host Bus Adapter
1	SWXKT-EA	UltraSCSI Hub Cluster RAID Connection Kit

2. Examine present configuration

Action	✔
Single path configuration functions properly – check event log on both servers	
Serial line connection available to the controller	
StorageSets and NT volumes defined – not hardware partitioned	
Windows NT system disk not part of RAID subsystem	
TCP/IP protocol installed on both Windows NT servers	
[Alpha servers] FX!32 not installed on either server	

3. Install Secure Path software

From the Secure Path CDROM, launch \SPINSTAL\SETUP.EXE on each server, and follow directions. Setup will shutdown the server. **Do not restart the server until you have completed preparing the RAID subsystem.**

4. Prepare the RAID subsystem

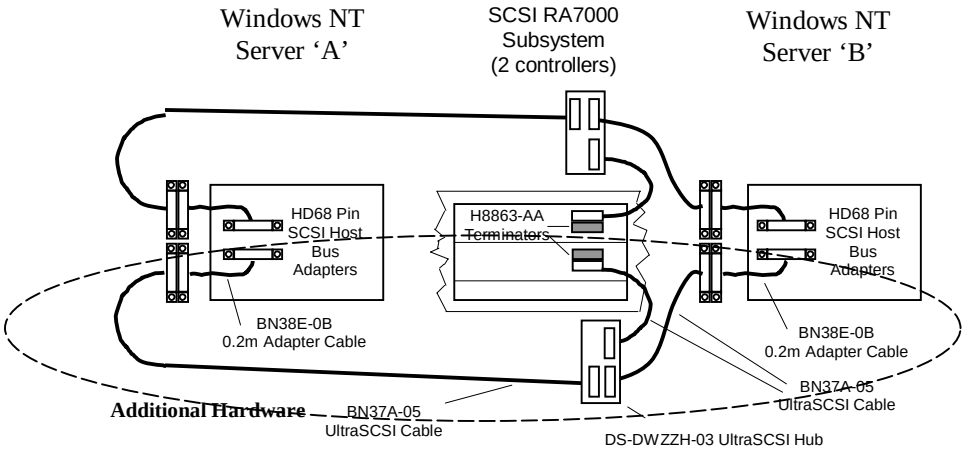
After the server has shutdown, perform the following actions:

Action	**Serial Line (CLI) steps**	✔
Set the controllers to multibus failover mode	HS***> **set nofailover** *The "other" controller will shutdown and must be manually restarted by momentarily depressing the reset button on the controller's front panel.* HS***> **set multibus copy=this** *The controllers will restart in multibus mode*	
Verify that the controller mode was changed to multibus failover.	HS***> **show this** HS***> **show other**	
Prefer each storage unit to "this" or the "other" controller.	HS***> **show units** HS***> **set** *(unit#)* **preferred=this** - or - HS***> **set** *(unit#)* **preferred=other**	

5. Install additional hardware

Adaptec AHA 2944UW Settings	✔
Internal termination **enabled**	
Host adapter BIOS **disabled**	
SCSI bus reset **disabled**	
Set unique SCSI Ids for each new adapter	

NOTE: You must assure that the connection between host adapters on both servers is consistent. Use the PCI slot numbering on your servers as a guide. The adapters on each server that connect to one controller should be in the same PCI slot in each server and must connect to the same hub. If it is not possible to install the adapters in the same slot in each server, you must install them in sequence. For example, the first adapters installed in each server must connect to the same controller.



6. Confirm installation

Action	✔
Reboot the servers	
Check event log for proper SCSI operation	
Launch Secure Path Manager	

Quick Setup Guide for

Fibre Channel RAID Array 8000 or ESA 12000 and one Windows NT server

Note: Do not install Secure Path for Windows in an Alpha server which has FX!32 installed.

1. Inventory additional components needed

Qty	Part Number	Description
1	QB-669AA-SA	Secure path for Windows (version 2 or higher)
1	KGPSA-BC	Fibre Channel Host Bus Adapter
1	DS-DHGGB-AA	Fibre Channel Hub
1	DS-DXGK2-SA	Fibre Channel Connection Kit 2 GBIC 2*2M

2. Examine present configuration

Action	✔
Single path configuration functions properly – check event log on server	
Serial line connection available to the controller	
StorageSets and NT volumes defined – not hardware partitioned	
Windows NT system disk not part of RAID subsystem	
TCP/IP protocol installed on Windows NT server	
[Alpha servers] FX!32 not installed on Windows NT server	

3. Install Secure Path software

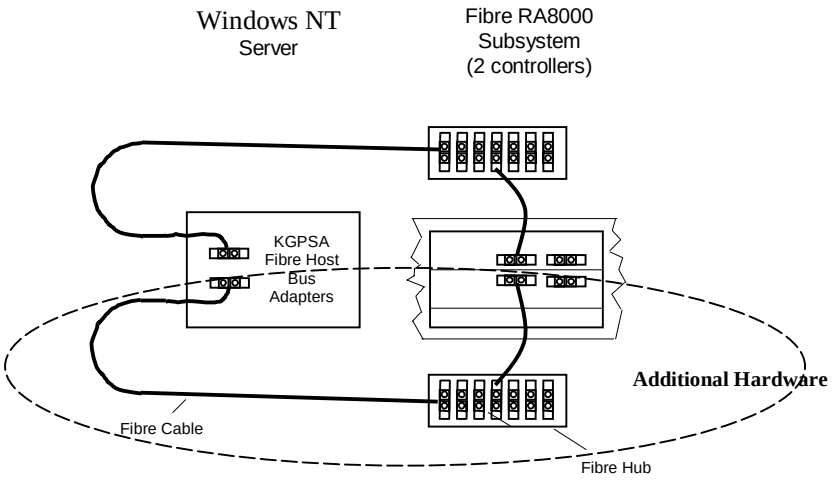
From the Secure Path CDROM, launch \SPINSTAL\SETUP.EXE on the server, and follow directions. Setup will shutdown the server. **Do not restart the server until you have completed preparing the RAID subsystem.**

4. Prepare the RAID subsystem

After the server has shutdown, perform the following actions:

Action	**Serial Line (CLI) steps**	✔
Set the controllers to multibus failover mode	HS***> **set nofailover** *The "other" controller will shutdown and must be manually restarted by momentarily depressing the reset button on the controller's front panel.* HS***> **set multibus copy=this** *The controllers will restart in multibus mode*	
Verify that the controller mode was changed to multibus failover.	HS***> **show this** HS***> **show other**	
Prefer each storage unit to "this" or the "other" controller.	HS***> **show units** HS***> **set** *(unit#)* **preferred=this** - or - HS***> **set** *(unit#)* **preferred=other**	

5. Install additional hardware



6. Confirm installation

Action	✔
Reboot the server	
Check event log for proper Fibre Channel operation	
Launch Secure Path Manager	

Quick Setup Guide for

Fibre Channel RAID Array 8000 or ESA 12000 and a Windows NT Cluster

Note: Do not install Secure Path for Windows in an Alpha server which has FX!32 installed.

1. Inventory additional components needed

Qty	Part Number	Description
1	QB-669AA-SA	Secure path for Windows (version 2 or higher)
2	KGPSA-BC	Fibre Channel Host Bus Adapter
1	DS-DHGB-AA	Fibre Channel Hub
1	DS-DXGK1-SA	Fibre Channel Connection Kit 2 GBIC 3*2M

2. Examine present configuration

Action	✔
Single path configuration functions properly – check event log on server	
Serial line connection available to the controller	
StorageSets and NT volumes defined – not hardware partitioned	
Windows NT system disk not part of RAID subsystem	
TCP/IP protocol installed on Windows NT server	
[Alpha servers] FX!32 not installed on Windows NT server	

3. Install Secure Path software

From the Secure Path CDROM, launch \SPINSTAL\SETUP.EXE on each server, and follow directions. Setup will shutdown the server. **Do not restart the server until you have completed preparing the RAID subsystem.**

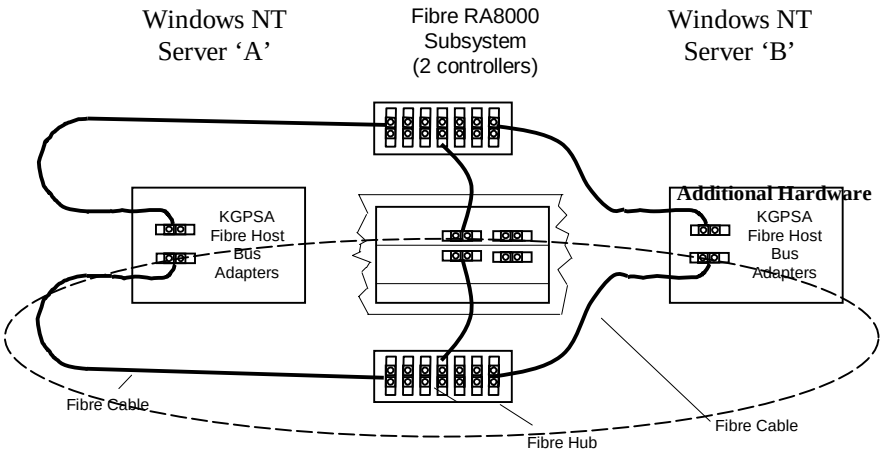
4. Prepare the RAID subsystem

After the server has shutdown, perform the following actions:

Action	**Serial Line (CLI) steps**	✔
Set the controllers to multibus failover mode	HS***> **set nofailover** *The "other" controller will shutdown and must be manually restarted by momentarily depressing the reset button on the controller's front panel.* HS***> **set multibus copy=this** *The controllers will restart in multibus mode*	
Verify that the controller mode was changed to multibus failover.	HS***> **show this** HS***> **show other**	
Prefer each storage unit to "this" or the "other" controller.	HS***> **show units** HS***> **set** *(unit#)* **preferred=this** - or - HS***> **set** *(unit#)* **preferred=other**	

5. Install additional hardware

NOTE: You must assure that the connection between host adapters on both servers is consistent. Use the PCI slot numbering on your servers as a guide. The adapters on each server that connect to one controller should be in the same PCI slot in each server and must connect to the same hub. If it is not possible to install the adapters in the same slot in each server, you must install them in sequence. For example, the first adapters installed in each server must connect to the same controller.



6. Confirm installation

Action	✔
Reboot the server	
Check event log for proper Fibre Channel operation	
Launch Secure Path Manager	

Comprehensive Installation Roadmap

StorageWorks Secure Path for Windows NT

- - - - - - - - - - - RoadMap - - - - - - - - - - -

STEP	PERFORM THIS PROCEDURE…	DESCRIBED IN…
❑ 1	**All Pre-Installation steps,** Including… ◊ Verify Secure Path Requirements ◊ Inventory the Secure Path Kits ◊ Prepare the RAID Array for Secure Path	*Secure Path for Windows NT* – Chapter 2
❑ 2	**Configure the RAID for Secure Path and Install the Secure Path Software**	*Secure Path for Windows NT* – Chapter 3
❑ 3	**Install the Secure Path Hardware**	*Secure Path for Windows NT* – Chapter 4
❑ 4	**Monitor and Manage the Secure Path Environment,** Using the Secure Path Manager to ◊ Check the Vitality of the Two SCSI Paths ◊ Check/Assign Disk I/O SCSI Paths ◊ Balance Disk I/O Between SCSI Paths ◊ Monitor Automatic Failover Activity ◊ Perform Manual Failback Activity	*Secure Path for Windows NT* – Chapter 5

After these steps have been successfully completed in sequence, the Secure Path configuration will be operational.

1

Theory of Operation

This section provides an overview of StorageWorks Secure Path for Windows NT.

An Overview of Secure Path for Windows NT

StorageWorks Secure Path is a high availability software product providing continuous data access for Ultra SCSI RAID Array 7000 / Enterprise Storage Array 10000 and Fibre Channel RAID Array 8000 / Enterprise Storage Array 12000 storage subsystems configured on Windows NT 4.0 Intel or Alpha platforms. Redundant hardware, advanced RAID technology and automated failover capability are used to enhance fault tolerance and availability. Secure Path effectively eliminates controllers, disk drives, interconnect hardware and host bus adapters as single points of failure in the storage subsystem.

Secure Path V2.0 allows a StorageWorks dual-controller RAID to be cabled on two independent SCSI busses or Fibre Channel loops, using two separate host bus adapters in each server.

Secure Path monitors each path and automatically re-routes I/O to the functioning, alternate path should an adapter, cable, hub or controller failure occur. Failure detection is reliable and designed to prevent false or unnecessary failovers. Failovers are transparent and non-disruptive to applications.

The Secure Path management utility provides continuous monitoring capability and identifies failed paths and failed-over storage units. To facilitate static load balancing, devices can be moved between paths using simple “drag-and-drop” operations.

Through use of dual RAID controllers configured in an active/active multibus mode of operation, Secure Path can also exploit the potential for improved data throughput and bandwidth performance.

Secure Path Technology

Key to Secure Path's functionality is the capability of dual StorageWorks RAID controllers to operate in an active/active implementation referred to as dual-redundant multibus mode. Multibus mode allows each controller to be configured on its own bus and to process I/O independently under normal operation. Available storage units are preferred to one or the other of the two controllers by setting a PREFERRED_PATH unit attribute. This attribute determines which controller path is used for access at system boot time. During runtime, units may be moved between paths at anytime through use of the Secure Path management utility.

Controllers in a dual-redundant multibus configuration monitor each other and automatically and transparently failover storage units from the failed member of a controller pair. The Secure Path software detects the failure of I/O operations to complete on a failed controller's path and automatically re-routes all traffic to the path of the surviving controller. Controller and path failover is completed seamlessly, without process disruption or data loss.

Following a warm-swap of a failed controller, adapter or cable component, storage units can be failed-back to their original path using the Secure Path management utility.

To protect against drive failure in a Secure Path environment, storage units can be configured using raid levels 0+1, 1, 3/5, or 5. Secure Path will support either FAT or NTFS file system formats on single host configurations. Microsoft requires the NTFS file system in Microsoft Cluster Server (MSCS) configurations.

Implementation

Secure Path's primary failover capability is implemented in a Windows NT filter driver called RaiDisk. RaiDisk provides support for the StorageWorks RAID subsystem multibus mode of operation and provides all functions required for monitoring I/O and detecting path failures. RaiDisk also filters the alternate path view to a storage unit so that application level programs and utilities, such as Explorer and Disk Administrator, report a logically consistent view of the underlying storage environment. RaiDisk uses custom event log entries to facilitate problem diagnosis and repair. Performance testing with Secure Path

installed demonstrates that there is less than a 0.5% performance reduction attributable to the RaiDisk driver.

Secure Path also incorporates the custom Windows NT class driver, HszDisk, developed for use with StorageWorks RAID Array controllers. This class driver provides unique error handling features and performance enhancements not available in the native Windows NT disk class driver.

Multi-path management is implemented using Secure Path Manager. Secure Path Manager is a client/server graphical application that continuously monitors the multi-path storage environment and automatically updates the displayed configuration information. Secure Path Manager indicates which path is currently servicing each configured storage unit. Online, offline, and pending state information for available storage units and paths is depicted using color codes. The capability to swap storage units between paths is also provided through simple "drag-and-drop" operations.

Installation and Configuration

A single host Secure Path configuration is comprised of a server, two host bus adapters, a StorageWorks RAID Array subsystem, and two sets of cables. A stylized Secure Path single server configuration is shown in Figure 1-1.

A Microsoft Cluster Secure Path configuration is comprised of two servers, two host bus adapters in each server, a StorageWorks RAID Array subsystem, and two sets of cables. A stylized Secure Path Microsoft Cluster configuration is shown in Figure 1-2.

All Secure Path software components are installed on either Intel or Alpha based platforms using the same InstallShield based setup utility. The setup procedure requires that a standard single path configuration be established, with all storage units defined, prior to installation of the Secure Path software. The Secure Path software is then installed on the single path configuration before re-configuration of the storage controllers for multibus mode and installation of hardware for the redundant path. This software-first/hardware-second procedure allows the operating system to properly configure the multi-path environment when rebooted.

For previously installed subsystems, no modifications are required to existing storage units or data volumes.

Figure 1-1 Secure Path Single Host Configuration

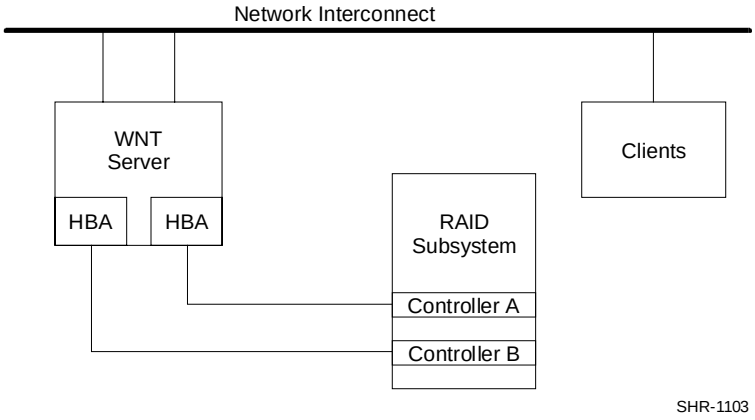
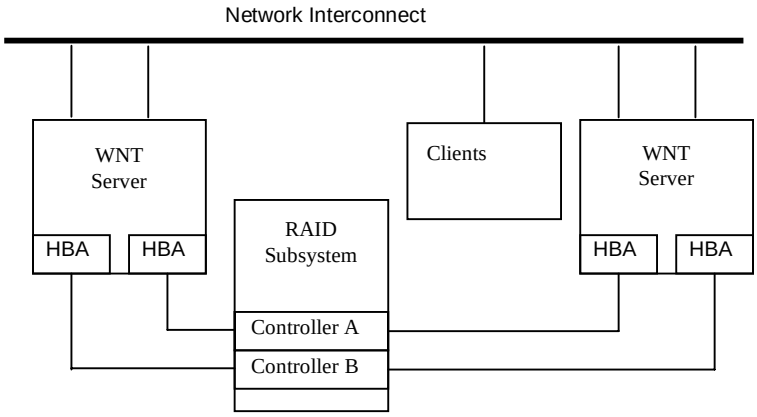


Figure 1-2 Secure Path Microsoft Cluster Configuration



The Secure Path Software (V2.0) for Microsoft Windows NT

The Secure Path Software Kit for Microsoft Windows NT is comprised of the following software components:

- **HszDisk.sys** is a Windows NT class driver that works with StorageWorks RAID Array controllers to enhance on-line storage availability and fault-tolerance. HszDisk works in single-host and cluster environments to maintain optimum subsystem performance during controller and storageset error recovery operations.

- **RaiDisk.sys** is a Windows NT filter driver that provides support for multibus mode operation with StorageWorks RAID Arrays. RaiDisk performs automatic failover of storagesets to the alternate path in the event of a primary path failure.
- **Secure Path Manager** is the client application used to manage multipath StorageWorks RAID Array configurations. Secure Path Manager displays a graphical representation of the current multipath environment and indicates the location and state of all configured storagesets on each of the paths. To facilitate static load balancing, Secure Path Manager provides the capability to move storagesets between paths. Secure Path Manager can be run locally at the managed servers, or remotely at a management workstation.
- **Secure Path Agent** is the server service that communicates with the RaiDisk filter driver on the server and with the Secure Path Manager on the client side via TCP sockets. The Secure Path Agent makes use of Windows NT application and event log and will post error and informational messages as required.
- **Secure Path Setup** supports driver installation and uninstallation with Windows NT 4.0.

2

Pre-Installation Steps

This section addresses the preparation needed before installing and configuring the Secure Path components.

2.1 Summary

The procedures described in this guide require that you have already installed your storage subsystem in a single host/single path configuration or a dual host cluster/single path configuration. It is further required that you have created storagesets on the subsystem using either the StorageWorks Command Console (SWCC) or Command Line Interface (CLI) and have also partitioned and formatted these drives with the Windows NT Disk Administrator. For complete information about setting-up your subsystem in a single path/single host environment please refer to the *Getting Started guide shipped with your StorageWorks Solutions platform kit.*

The pre-installation steps required to support a Secure Path environment are:

- Verify the Secure Path Requirements
- Inventory the StorageWorks Kits Required for Secure Path
- Prepare the RAID Array for Secure Path Operation

2.2 Verify the Secure Path Requirements

Please verify that the Secure Path requirements listed in Table 2-1 are met.

Table 2–1 Secure Path Prerequisites

Host Feature	Requirement
Platform	One or two (Intel or Alpha) host server(s)
Operating System	Microsoft Windows NT, Version 4.0, SP3 -or- Microsoft Windows NT Enterprise Edition
Secure Path Software	StorageWorks Secure Path Software Kit V2.0 for Windows NT (Kit # QB-669AA-SA)
RAID Storage Subsystem	At least one StorageWorks dual-redundant UltraSCSI RA7000 / ESA10000 or Fibre Channel RAID Array 8000 or ESA12000 installed and configured for single path operation.
SCSI Host Adapters (and adapter driver)	Two identical Host Adapters Supported models: Adaptec AHA-2944UW (for Intel or Alpha servers) StorageWorks KGPSA (for Intel or Alpha servers)

Table 2–1 Secure Path Prerequisites (cont)

Additional Items	Requirement
Interconnect Hardware	As required
RAID Hardware	Cables supplied with host RAID Array Platform kit
Service Tools	Appropriate tools to service your equipment
Technical Documentation	The reference guides for your RAID subsystem, the host server and the Windows NT software supplement this installation guide.

NOTE

With the exception of controller-based partitioning and system boot disk support, all RAID Array features supported for single path environments are also supported with multipath environments.

2.3 Inventory the StorageWorks Kits Required for Secure Path

Please verify that you have received the following StorageWorks Secure Path hardware and software installation kits that may be appropriate to your installation:

1. For SCSI RAID Array 7000 or ESA 10000 with one Windows NT Server

QTY.	PART NO.	DESCRIPTION
1	QB-669AA-SA	Secure Path for Windows
1	AHA2944UW	UltraSCSI host adapter
1	SWXKT-FA	RAID SCSI Connection Kit

2. For SCSI Raid Array 7000 or ESA 10000 with Windows NT Clusters and Y-cables.

QTY.	PART NO.	DESCRIPTION
1	QB-669AA-SA	Secure Path for Windows, version 2
2	AHA2944UW	UltraSCSI host adapter
1	SWXKT-DF	Cluster RAID Connection Kit

3. For SCSI Raid Array 7000 or ESA 10000 with Windows NT Clusters and SCSI hubs.

QTY.	PART NO.	DESCRIPTION
1	QB-669AA-SA	Secure Path for Windows, version 2
2	AHA2944UW	UltraSCSI host adapter
1	DS-DWZZH-03	UltraSCSI 3-port Hub
1	SWXKT-EA	UltraSCSI Hub Cluster RAID Connection Kit

4. For Fibre Channel Raid Array 8000 or ESA 12000 with one Windows NT Server

QTY.	PART NO.	DESCRIPTION
1	QB-669AA-SA	Secure Path for Windows, version 2
1	KGPSA-BC	Fibre Channel host adapter
1	DS-DHGGB-AA	Fibre Channel Hub
1	DS-DXGK2-SA	Fibre Channel Connection Kit GBIC 2*2M

5. For Fibre Channel Raid Array 8000 or ESA 12000 with Windows NT Clusters

QTY.	PART NO.	DESCRIPTION
1	QB-669AA-SA	Secure Path for Windows, version 2
2	KGPSA-BC	Fibre Channel host adapter
1	DS-DHGGB-AA	Fibre Channel Hub
1	DS-DXGK1-SA	Fibre Channel Connection Kit GBIC 3*2M

If you are missing any component required for your Secure Path environment, please contact your local sales representative or call the StorageWorks Resource Center at 1-800-STORWOR (1-800-786-7967) before proceeding.

2.4 Examine the current configuration

The next step is to assure that the existing single path configuration conforms to Secure Path requirements. The requirements are as follows:

Existing storage infrastructure must be robust –

a) Verify that there is a serial connection to the storage subsystem and that you can communicate to it via SWCC or the CLI.

b) Launch the NT event log viewer and check to see that HSZdisk is installed and that it reports the expected number of logical units.

c) Check the NT event log viewer and determine that there are no error events reported by the host adapter or HSZdisk.

d) Verify that the Windows NT system (boot) disk is not part of the storage subsystem

e) Verify that none of the LUNs are partitioned by the storage controller hardware.

f) Verify that none of the NT volume sets use software RAID or use extended volumes.

g) Verify that the server has the TCP/IP protocol installed and that the server is available on the network by pinging it.

h) **Verify, for Alpha servers only, that FX!32 is not installed or is disabled**.

i) Verify that, for Alpha servers using Adaptec 2944UW host bus adapters, the server is using aic78xx.sys driver version 2.11S30 or higher.

2.5 Prepare the RAID Array for Secure Path Operation

The procedures to prepare your RAID Array for a Secure Path environment (described in this section), depend upon whether you are converting an existing RAID Array to Secure Path operation or are installing a brand new subsystem.

WARNING

If you currently have a RAID Array in a production environment, which is being converted to Secure Path operation, make sure that all users have logged off the server and that all I/O to the RAID subsystem has ceased before proceeding.

2.5.1 Preparing an Existing RAID Array for Secure Path Operation

If you have an existing RAID Array that is currently being used in a production environment and plan to reconfigure for Secure Path operation, you should perform the following steps before proceeding to Chapter 3:

1. Follow normal procedures to backup the data stored on all drives configured on the RAID Array.
2. Check that your RAID Array subsystem does not make use of controller-based partitioning. Partitioned storagesets and partitioned single-disk units are not supported in multibus failover, dual-redundant configurations. Re-configure to eliminate any controller-based partitions.

WARNING

Before you delete any partitions on the RAID Array, backup your data and then use Windows NT Disk Administrator to delete the partition(s) from the drives before you delete the storage unit(s) from the RAID Array configuration.

2.5.2 Preparing a New RAID Array for Secure Path Operation

If you have a new RAID Array that will be configured for Secure Path operation, you should perform the following steps before proceeding to Chapter 3:

1. Install the RAID Array in a single path configuration according to the installation documentation you received with the platform kit.
2. Use StorageWorks Command Console (SWCC) or CLI to establish the desired storageset configuration. Do not use controller-based partitions in your RAID Array configuration.
3. Use Windows NT Disk Administrator to partition and format the storagesets.

3

Installing Secure Path Software

This chapter describes the software configuration procedures required to establish Secure Path operation to a RAID Subsystem.

3.1 Summary

The following sections describe the software configuration procedures required for your Secure Path storage environment, which are as follows:

- Install the StorageWorks Secure Path software on the host server(s)
- Establish a serial link to the RAID subsystem
- Set RAID controllers to multibus failover mode
- Prefer the paths of the storagesets (units) to the RAID controllers

After performing these procedures in sequence, the software configuration of your Secure Path storage environment will be complete.

3.2 Installing the Secure Path Software

3.2.1 Description of the Secure Path Software

Secure Path for Windows consists of a kernel mode driver 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 for Windows is managed by a client/server management application which requires that TCP/IP be installed in the Windows NT server attached to the Storage where the Secure Path agent is installed; and on the management station on which the Secure Path Manager graphical user interface is installed.

The Secure Path user interface and agent (client/server) may be installed in the same server, as long as the agent is installed on the server that is attached to the storage subsystem to be managed.

3.2.2 Installing the Secure Path driver and agent

The following section describes how to install the Secure Path drivers and configuration management agent on the host server.

1. Insert the *StorageWorks Secure Path Software (V2.0) for WNT* distribution CD in your CD-ROM driver.
2. If you have CD AUTORUN enabled on your server; the Secure Path setup program will start automatically. Otherwise, Choose "Run" from the START menu and enter the command shown below, substituting your CD-ROM's drive letter for the one shown.

   Drive_Letter:\SPINSTAL \SETUP.EXE

   When the setup starts, choose the **server** install option. The server option will install the drivers and the agent required by Secure Path.

   Be prepared to designate those clients that you wish to allow to manage the host. These names have to be fully qualified, for example "myserver.mydomain.com". There are many ways to configure TCP/IP on your network. They include a) host files on servers and clients and b) DNS, with NetBios using DNS resolution. Check with your system administrator to assure proper network configuration.
3. Make sure to enter a validation password. For cluster configurations make sure the password is the same for each member of the cluster.

3.2.3 Installing the Secure Path Manager

The following section describes how to install the Secure Path management application on the management station. The management application can be installed on the host server, or on a separate management station.

1. Insert the *StorageWorks Secure Path Software (V2.0) for WNT* distribution CD in your CD-ROM driver.
2. If you have CD AUTORUN enabled on your server; the Secure Path setup program will start automatically. Otherwise, Choose "Run" from the START menu and enter the command shown below, substituting your CD-ROM's drive letter for the one shown.

   Drive_Letter:\SPINSTAL \SETUP.EXE

When the setup starts, choose the **client** install option. The client option will install the Secure Path Management graphical user interface.

3.3 Establishing a Serial Link to the RAID Subsystem

While StorageWorks Command Console (SWCC) may be used to define and configure storagesets on the subsystem, it cannot be used to establish a Secure Path environment. Thus, the Command Line Interface (CLI) must be used to configure the controllers for multibus mode operation. Controller status may be obtained through use of the SWCC CLI Window or a terminal emulation program via serial connection.

Use StorageWorks Command Console (serial connection/CLI Window) or a terminal emulation program such as *Hyperterminal* to establish a serial connection to the subsystem. You will use this connection to issue "CLI" commands to the subsystem.

You may use a serial line connection from the host server or from any PC workstation. Please refer to the *Command Console 2.0 User's Guide* or the *Getting Started Guide* shipped with your platform kit for information on how to setup and use a serial connection and the "CLI Reference Manual" for complete information on CLI commands and syntax.

3.4 Configuring the RAID Subsystem for Secure Path Operation

This section describes how to configure the RAID subsystem controllers for a Secure Path environment, which includes:

- Setting the controllers to multibus failover mode
- "Preferring" (specifying) which RAID controller (SCSI bus path or Fibre Channel loop) the I/O of each disk will be assigned to upon system boot.

NOTE

Partitioned storagesets and partitioned single-disk units (controller-based partitioning) cannot function in multiple bus failover dual-redundant configurations. Because they are not supported, you must delete and re-configure these storagesets before configuring the controllers for multiple bus failover. Make sure you use Windows NT Disk Administrator to delete partitions on drive(s) before you delete the corresponding storageset(s).

3.4.1 Setting HSZ70 or HSG80 Controllers to MultiBus Failover

Secure Path operation requires that the RAID controllers be configured for multiple bus failover mode through use of the Command Line Interface (CLI). This is accomplished by **issuing four individual commands, in the sequence provided in this section**, at the CLI prompt. For clarity, the command lines are presented in bold text, and followed by a description of the action produced or required after each command is issued.

HS*** > **set nofailover**

The "other" controller will shutdown and must be manually restarted by momentarily depressing the reset button on the controller's front panel. ***Wait for 2 minutes for the controller to boot before proceeding.***

HS*** > **set multibus copy=this**

The controllers will restart in multibus mode.

After the other controller has restarted, verify that both controllers are configured for multibus mode by issuing the following commands:

HS*** > **show this**

HS*** > **show other**

The controllers are now configured for multibus operation.

3.4.2 "Preferring" Storage Unit Paths

To complete the multibus configuration setup, you must "prefer" (assign) storage units to one or the other controller to specify which controller is used to access units at system boot time. The preferred_path unit attribute assigns units to either "this" or the "other" controller. In effect, this procedure specifies on which path (controller, SCSI bus, and host adapter) the I/O will travel.

Initially, it is recommended that you balance the available storagesets between the busses. As storage demands are defined and individual drive throughput requirements are understood, adjustments to the disk I/O path configuration may be made using the StorageWorks Secure Path Manager, as described in Chapter 5 of this guide.

Use the following command to obtain a list of all units defined in the RAID subsystem:

HS***> **show units**

Use the following command to specify PREFERRED_PATH for units:

HS*** > **set** *(unit #)* **preferred=this**

- or -

HS*** > **set** *(unit #)* **preferred=other**

Repeat for each configured storage unit in your configuration

You have completed the software configuration required to support your Secure Path environment. Proceed to Chapter 4 to cable the second path. Then you will be ready to monitor and manage Secure Path activity using the StorageWorks Secure Path Manager, as described in Chapter 5 of this guide.

4

Installing Secure Path Hardware

This chapter provides the procedures for installing and terminating a second individual I/O path between a StorageWorks RAID subsystem and an NT host server or a Microsoft Cluster Server, where currently a single I/O path exists.

WARNING!

Follow normal procedures to power off your server prior to cabling.

4.1 Summary

Configuring Secure Path hardware components consists of three main tasks to be performed in sequence, as described in the following sections.

1. Prepare and Install the Second Host Adapter
2. Cable the Secure Path Hardware Components
3. Verify the Secure Path Hardware Configuration

4.2 Prepare and Install the Second Host Adapter

To complete your Secure Path installation you must install a second host adapter (HBA) in the server(s).

Prior to *installing* the second host adapter into the server, the host adapter must be *prepared* for Secure Path operation.

For SCSI Adaptec AHA2944UW host adapters:

- Setting/Verifying SCSI Host Adapter Termination
- Disabling SCSI Bus Reset
- Disabling SCSI Host Adapter BIOS

For Fibre Channel KGPSA host adapters:

- No preparation required

4.2.1 Setting Up SCSI Host Adapters

Refer to the documentation supplied with your adapter to help you configure the following parameters. Make sure that these settings are identical for each host adapter.

For SCSI host adapters:

1. Termination is **enabled** unless you are using Y-cables with external termination. If you are using Y-cables with external termination then you must **disable** termination on the host bus adapter.
2. SCSI bus resets following board initialization (power-on reset) are **disabled.**
3. SCSI host adapter BIOS is **disabled**.

The host adapters are now prepared for Secure Path operation. Follow the adapter vendor's recommended procedure to install the second adapter in your server's system bus.

4.3 Installing Cables and Termination

Choose from one of the following subsections to properly cable your Secure Path configuration:

If you are installing a SCSI RAID Array 7000 or ESA 10000 and one Windows NT server, choose section 4.3.1

If you are installing a SCSI RAID Array 7000 or ESA 10000 and a Windows NT Cluster with SCSI Y-cables, choose section 4.3.2

If you are installing a SCSI RAID Array 7000 or ESA 10000 and a Windows NT Cluster with SCSI Hubs, choose section 4.3.3

If you are installing a Fibre Channel RAID Array 8000 or ESA 12000 and one Windows NT Server, choose section 4.3.4

If you are installing a Fibre Channel RAID Array 8000 or ESA 12000 and a Windows NT Cluster, shoose section 4.3.5

4.3.1 Installing a SCSI RAID Array 7000 or ESA 10000 and one Windows NT server

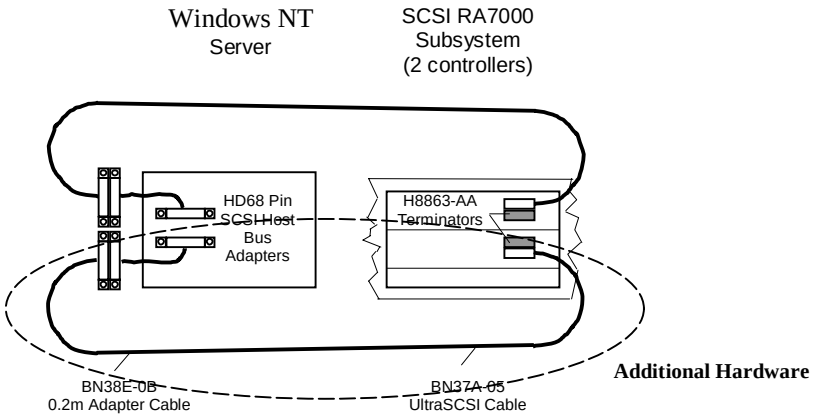
To establish two individual SCSI busses between a single Windows NT host server and a RAID subsystem, where one bus exists, reference Figure 4-1 and follow these steps:

1. Install the Host Bus Adapter in the server.
2. Remove the link cable interconnecting both HSZ70 RAID controllers in the storage subsystem.

3. Connect a terminator (H8863-AA) to the remaining tri-link connector of the controller that is currently connected to the host server.
4. Attach (the compatible) end of the UltraSCSI cable (BN37A-05) to the tri-link connector on the controller in the RAID subsystem that is not currently connected to the host server.
5. Connect (the compatible) end of the .2M adapter cable (BN38-E-0B) to the available end of the UltraSCSI cable.
6. Attach the other end of the .2M adapter cable to the available SCSI host adapter board resident in the host server.
7. Verify that the terminator (H8863-AA) pre-existing in the newly-cabled controller is firmly attached into its tri-link connector.
8. Reboot the host server.

The Secure Path solution is now properly prepared, cabled and terminated.

Figure 4–1 Secure Path Hardware Interconnect – SCSI Single Server



NOTE

In Figure 3-1, notice that the link cable between the two RAID controller boards has been removed, and that both busses are terminated on the controller.

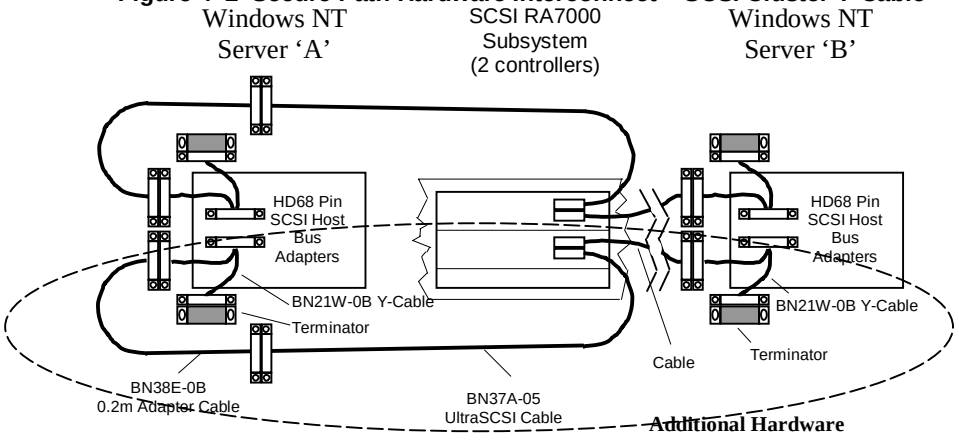
4.3.2 Installing a SCSI RAID Array 7000 or ESA 10000 and a Windows NT Cluster with Y-Cables.

To establish two individual SCSI busses between clustered Windows NT host servers and a RAID subsystem, where one bus exists, reference Figure 4-2 and follow these steps:

1. Install the Host Bus Adapter in the servers.
2. Remove the link cable interconnecting both HSZ70 RAID controllers in the storage subsystem.
3. Remove both VHDCI terminators from the controllers.
4. Move one of the existing VHDCI cables from the bottom controller to the top controller. Both connectors on the bottom controller should now be unused.
5. Attach Y-cables to each of the new host bus adapters, one new adapter in each server.
6. Attach SCSI terminators to one end of each Y-cable.
7. Attach the (compatible) end of the .2M adapter cable (BN38E-0B) to the available end of the Y-cable of one server, and extend it to the bottom controller using the 5 meter VHDCI cable (BN37A-05)
8. Attach the VHDCI/HD68 5 meter cable between the remaining Y-cable and the bottom controller.
9. Reboot the host server.

The Secure Path solution is now properly prepared, cabled and terminated.

Figure 4–2 Secure Path Hardware Interconnect – SCSI Cluster Y-Cable



NOTE
In Figure 4-2, notice that the link cable between the two RAID controller boards has been removed.

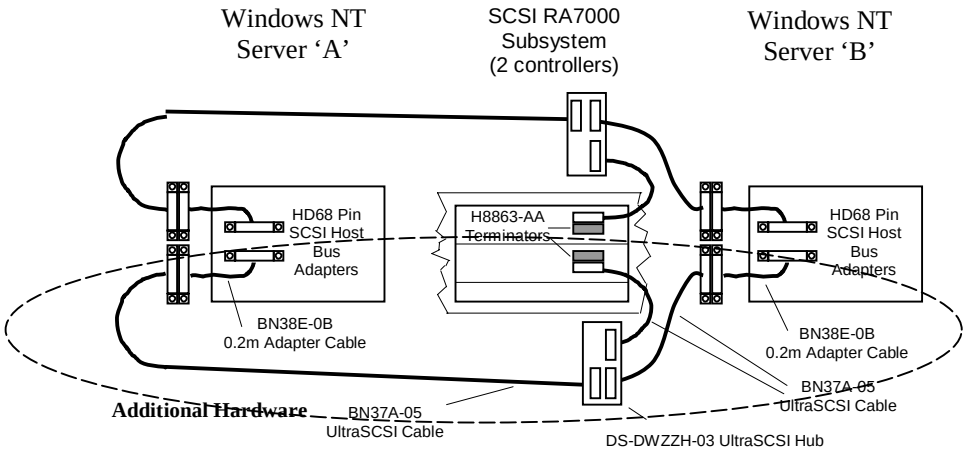
4.3.3 Installing a SCSI RAID Array 7000 or ESA 10000 and a Windows NT Cluster with SCSI Hubs.

To establish two individual SCSI busses between clustered Windows NT host servers and a RAID subsystem, where one bus currently exists, reference Figure 4-3 and follow these steps:

1. Install the Host Bus Adapter in the servers.
2. Remove the link cable interconnecting both HSZ70 RAID controllers in the storage subsystem.
3. Install a VHDCI terminator on the both controllers (one already has a terminator installed)
4. Attach the (compatible) end of the .2M adapter cable (BN38E-0B) to the host bus adapters, and extend it to a SCSI hub using the 5 meter VHDCI cable (BN37A-05)
5. Connect the remaining port of the 3 port SCSI hub to the RAID Array controller.
6. Reboot the host server.

The Secure Path solution is now properly prepared, cabled and terminated.

Figure 4–3 Secure Path Hardware Interconnect – SCSI Cluster Hub



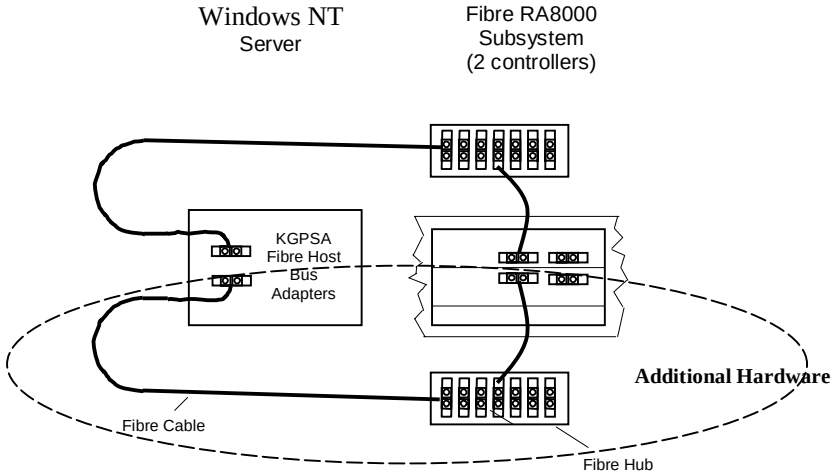
4.3.4 Installing a Fibre Channel RAID Array 8000 or ESA 12000 and one Windows NT Server

To establish two individual Fibre Channel loops busses between a single Windows NT host server and a RAID subsystem, where one bus currently exists, reference Figure 4-4 and follow these steps:

1. Install the Host Bus Adapter in the server
2. Connect the second hub to the second host bus adapter and to the second controller. **Note – You must use only one set of ports in the controller pair**.
3. Reboot the host server.

The Secure Path solution is now properly prepared and cabled.

Figure 4–4 Secure Path Hardware Interconnect – Fibre Channel Single Server



4.3.5 Installing a Fibre Channel RAID Array 8000 or ESA 12000 and a Windows NT Cluster

To establish two individual Fibre Channel loops between clustered Windows NT host servers and a RAID subsystem, where one bus currently exists, reference Figure 4-5 and follow these steps:

1. Install the Host Bus Adapters in the servers
2. Connect the second hub to the second host bus adapter in each server and to the second controller. **Note – You must use only one set of ports in the controller pair**.
3. Reboot the host server.

The Secure Path solution is now properly prepared and cabled.

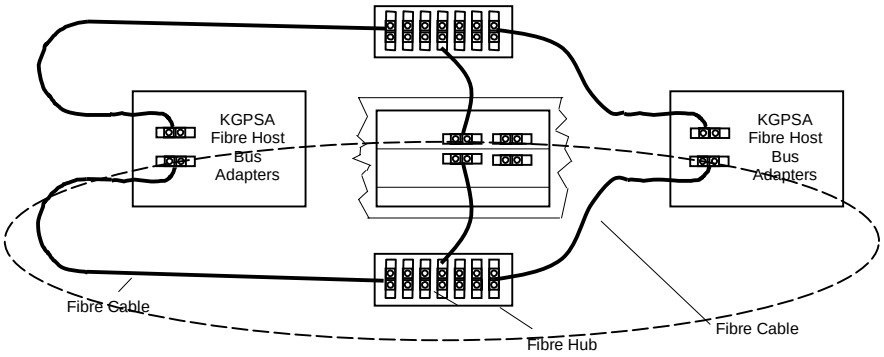


Figure 4–5 Secure Path Hardware Interconnect – Fibre Channel Cluster

4.4 Verify the Secure Path Hardware Configuration

Following system reboot, check the Windows NT system event log for successful start events for the RaiDisk and HszDisk drivers.

5

Using StorageWorks Secure Path Manager

This chapter describes how to use StorageWorks Secure Path Manager to monitor and manage a StorageWorks Secure Path for Windows NT environment.

5.1 About StorageWorks Secure Path Manager

NOTE

This chapter assumes that RAID Array storagesets have already been configured using SWCC or CLI and that the drives have been partitioned and formatted with Windows NT Disk Administrator. These procedures are described in the *Getting Started* guide shipped with your subsystem.

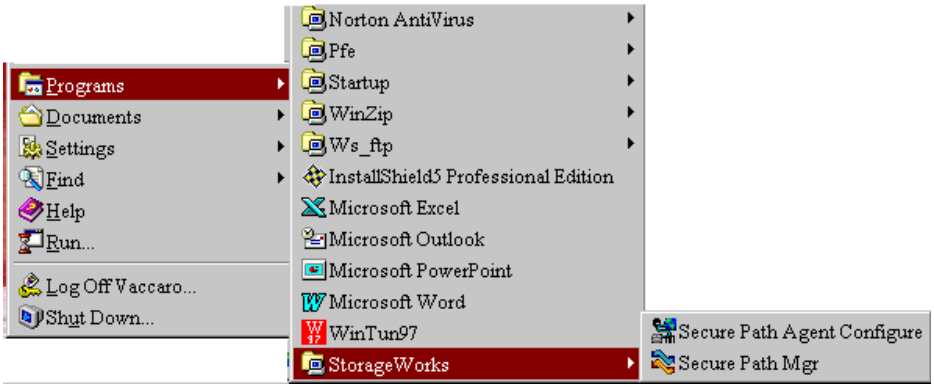
StorageWorks Secure Path Manager is a Graphical User Interface (GUI) utility that:

- Reports the status of the two paths
- Facilitates balancing I/O between the two bus paths
- Reports disk status (path assignment, failover, and failback activity)
- Enables (manual) drive failback upon path restoration

It is recommended that Secure Path Management application remain active (or minimized), to provide continuous Secure Path status monitoring. To monitor and manage a Secure Path environment using Secure Path Manager as described in the following sections, reference Figure 5-1 and proceed as follows:

1. From the START menu, select the Programs\ Secure path submenu.
2. Double-click on the Secure Path Manager application ICON.

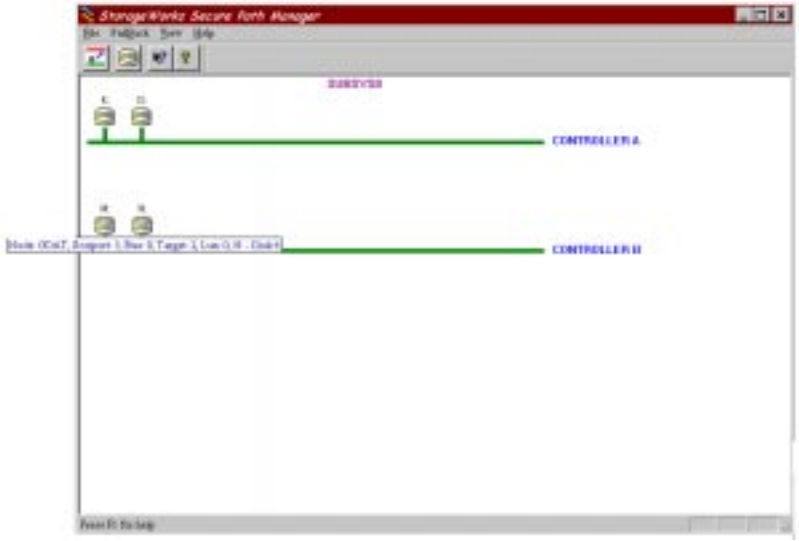
Figure 5–1 Invoking Secure Path Manager



5.2 Path and Drive Status Monitor

The Secure Path Manager screen appears as shown in Figure 5-2. The two paths (Path 0 and Path 1) are displayed *green* by the Manager when both paths (host adapters, cabling and controllers), are functioning normally. The Manager keeps track of the *primary path* (bus assignment) for each disk in the RAID subsystem. When operating normally, the Manager displays each disk on the primary path to which it has been assigned, as a disk icon, shaded *yellow and gray*. If a drive letter has been assigned to the disk, it will be displayed above the disk icon.

Figure 5–2 Typical Secure Path Manager Display



Determining Disk Identity

Drives configured in a MultiPath environment may be identified three ways. If you hover the cursor over a disk icon, The Manager will display the various identities of a drive – port/bus/target/lun and disk #. You may also view this information by right-clicking the mouse on the disk icon to launch the properties dialog for the drive. The port/bus/target/lun information refers to the physical identity of the drive's corresponding storageset (unit) as designated by the RAID Array subsystem. The disk # refers to the number assigned to a drive by Windows NT's Disk Administrator and the drive letter, appearing above the drive icon, is assigned to that partition (if one exists) by the System Administrator. If a drive has more than one partition they will appear above the drive as well. This drive information should allow you to quickly map storageset to operating system identity and determine which storagesets are currently serviced through each path.

5.3 Assigning New Primary Paths to Drives

To assign a new primary path to a drive using the Manager, proceed as follows:

1. Use the left mouse key to select the icon of the disk that is to receive a new primary path assignment (the icon will become a null-circle when selected).
2. Drag the disk icon from its current primary path to the alternate path displayed on the screen (the icon turns gray while in transition and the cursor changes to a squared arrow).
3. Drop the disk icon, anywhere you see the squared arrow along the "new" primary (formerly alternate) path, by releasing the mouse key.

When the primary path re-assignment of a disk completes, its icon will appear in its original form, shaded *gray and yellow*, on the new path. (It may appear above or beneath the path line, depending on your exact placement of the mouse). Repeat this procedure for each disk that is to be assigned a new primary path. A maximum of 24 drives can be assigned between both paths.

The Manager will not permit a new primary path assignment to a failed path. If an attempt is made to move a drive to a failed path the Manager will return the drive to the original path. A popup will also appear stating that the failback was not successful.

NOTES

The order and spacing of the disk icons displayed on the paths is refreshed every 90 seconds, and can be refreshed immediately using the View/Refresh pull-down menu of the Manager window or by depressing the F5 hot key.

5.4 Balancing the I/O Load Between Paths

As the storage demands of your Secure Path environment are defined and individual drive throughput requirements are understood, it is recommended that the disks generating the highest I/O loads be evenly balanced between the two paths to maximize overall throughput. The Manager may be used to statically load balance your Secure Path configuration by following the procedure noted below.

1. Identify "hot" drives - those that consistently experience the greatest I/O load while running workloads typical of your production environment. Enable Windows NT disk performance statistics, if you have not done so already, by issuing "**diskperf –y**" from a command window and restarting your system. Next, use Windows NT Performance Monitor to characterize individual drive loading in terms of throughput (I/O's per second) and/or

bandwidth (bytes per second), whichever is more appropriate for your application.
2. Note the path assignments of hot drives.
3. Balance the overall I/O load by evenly distributing (reassigning drive primary path), as much as possible, the hot drives between the two paths. Run your workload, monitor, and re-adjust as necessary.

Reference Section 5.3 for the procedures to assign a new primary path to a drive using the Manager.

5.4.1 Defining a Persistent Secure Path RAID Array Drive Configuration

When the primary path for a drive is changed using the Manager, the *preferred_path* (refer to section 2.3.2) assignment for the corresponding storage unit on the RAID Array does not change. If the *preferred_path* is not changed to the new path, the unit will revert to its original *preferred_path* if both the RAID Array and host server are power cycled together. To make the primary path assignment persistent for those drives you have reassigned with the Manager, re-set the *preferred_path* attribute for the corresponding storage unit on the RAID Array. Use the following procedure:

1. Use the CLI command **show units** to show the *preferred_path* settings for all units. This command will also indicate which controller each storageset is currently online with ("this" or "other).
2. Next, use the CLI command **set *unit#* preferred=this/other** to change the preferred path attribute to the appropriate path. For instance, if a storage unit is reported as being "online to ***other*** controller" but is preferred to the "***this***" controller, then you should change the **preferred_path** attribute to the "***other***" controller.
3. Repeat this procedure for each storage unit that is online to a path that is not its preferred path. It is not necessary to restart your server or RAID Array to perform this procedure.

5.5 Automatic Failover

When a path fails, (Secure Path software detects the loss of drive I/O due to adapter, cable or controller malfunction), the Secure Path software will:

- Perform an automatic failover and move the effected drive/s to the alternate path.
- Log failover event/s in the Windows NT system Event Log.
- Report the path failure via Windows pop-up message.

- Reflect the drive/s reassignment to the failover path on the display.

> **NOTE**
>
> Check the Windows NT system Event Log for entries generated by the Secure Path software to help in determining which component(s) of the path have malfunctioned. Look for entries by the HszDisk and RaiDisk drivers.

5.5.1 Automatic Failover Detection and Status Reporting

The Secure Path software continuously monitors the operational status of drives configured on each path. If the Secure Path software detects the failure of an I/O to complete for a drive, it will immediately move that drive to its alternate path and reroute outstanding I/O accordingly. Following the occurrence of any drive failure, the Manager will reflect the updated Secure Path configuration within its 90 second refresh interval, or sooner if the user depresses the F5 key.

When the Manager discovers the failover of at least one drive, it generates a Windows pop-up message and designates the path as failed by changing its color from green to yellow. Because the Secure Path software detects path failure through failed I/O operations, *only those drives with I/O active at the time of the failure will failover*. Those without active I/O will remain on the failed path until I/O is generated to them or they are moved manually to the failover path by a drag-and-drop operation. When all drives have been failed-over, the Manager will color the failed path red.

As shown in Figure 5-3, a failover is indicated by the Manager in three ways:

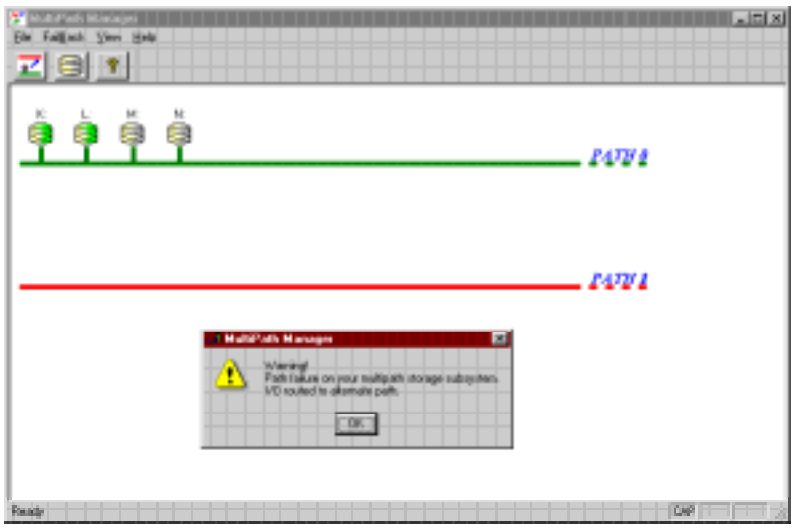
1. The failed path changes from green to *red*, or *yellow* if inactive drives remain on the path.
2. The effected disk icons relocate from their primary path to the alternate path, indicating that disk I/O has been failed-over to the alternate path.
3. On the alternate path, the disk icons that have been failed-over from their primary path reappear, shaded *green*.
4. A Windows pop-up message appears to report the failure.

NOTES

For a quick reference of the disk colors and their meaning, select *Legend* from the "VIEW" pull-down menu. The three possible drive states are identified and displayed in color.

Reference the Help files for possible path colors and states.

Figure 5–3 Automatic Disk Failover from Failed Path 1



COLORS FOR FIGURE 5-3:

- The failed path (Path 1) turns *red*, (or *yellow* if inactive disk/s remains on it).
- The failed-over disks appear *green* on their alternate path (Path 0).

5.6 Manual Failback and Status Reporting

Once a failed path is restored, the disks that had been failed-over to an alternate path must be failed-back manually, one at a time. As a safeguard, the Manager *does not automatically failback* drives. Rather, it enables disks to be *manually* failed-back, once the administrator validates the integrity of the path.

NOTE

For a failed path to return to the normal (green) state, the path must be restored and one or both of the following events must occur:

- All of the failed-over disks are failed back to it.
- The NT server is rebooted.

Failed-over drives may be restored to their primary path using one of the four failback methods described in this section

Failback Methods

- Failback Method 1: Double-click on the disk (icon) to be failed-back.
- Failback Method 2: From the "FAILBACK" pull-down menu, select the Failback option; select the disk, then click "OK".
- Failback Method 3: In the Manager Toolbar, click on the failback button (white button with an arrow and red line); select the disk, then click "OK".
- Failback Method 4: Drag-and-Drop each failed-over disk icon to its primary path, as follows:

    1. Use the left mouse key to select the icon of the disk that is to failback to its assigned primary path (the icon will become a null-circle when selected).
    2. Drag the disk icon from its current, alternate path to the primary path displayed on the screen (the icon turns gray while in transition, and the cursor changes to a squared arrow).
    3. Drop the disk icon anywhere along the disk's primary path by releasing the mouse key.

If more than one drive requires failback, repeat these steps until all the drives are failed-back, and the restored path turns green. As each individual drive returns to its primary path, the drive icons will return to their normal *yellow and gray* color. (The disk icon may appear above or beneath the path line, depending on your exact placement of the mouse). The failback path's color will not return to green until all failed-over drives have been restored to their primary path.

NOTE

The order and spacing of the disk icons displayed on the paths can be refreshed using the

View/Refresh pull-down menu of the Manager window or by depressing the F5 key.

5.7 Adding New Storagesets with Secure Path

To add new storagesets to a Secure Path configuration, proceed as follows:

1. Use StorageWorks Command Console (SWCC) or CLI to create a new storageset/s on the RAID Array.
2. Use CLI to assign a preferred path to the new unit, as described in Section 3.3.2.
3. Use appropriate procedures to add a new volume to the NT server or cluster.
4. Restart the host server(s) so that Windows NT and the Secure Path software can configure the new unit.

5.8 Removing a Storageset with Secure Path

1. Use Windows NT Disk Administrator to delete the partition from the drive to be removed using appropriate procedures.
2. Shutdown Windows NT on the host server(s).
3. Use StorageWorks Command Console (SWCC) or CLI to delete the storageset/s on the RAID Array.
4. Reboot the host server(s) to allow the Secure Path software to configure storage devices.

A

De-Installing Secure Path Software

This appendix describes how to remove StorageWorks Secure Path software from your server as required to resume a single path RAID storage environment.

A.1 How to De-Install StorageWorks Secure Path Software

To remove Secure Path software from your system, perform the following steps:

1. Establish a serial connection to the storage subsystem (as described in Chapter 2, Section 2.2).
2. Issue the de-installation commands (in bold text) below. (The commands are followed by a description of the action that is produced or required upon issuance).

   HSZ70> **set nomultibus**

   The other controller will shutdown. Momentarily depress the restart button on the controller's front panel to restart the controller. Wait for the controller to restart before proceeding to the next command.

   HSZ70> **set failover copy = this**

   The controllers will configure for dual-redundant operation.
3. Launch the WNT control panel and choose "Add/Remove Programs".
4. Select "Remove StorageWorks RaiDisk", and click OK to the resulting window.
5. Select "Remove StorageWorks Secure Path Manager", and click OK to the resulting window.
6. Select "Remove StorageWorks Secure Path Agent", and click OK to the resulting window
7. **For Fibre Channel RAID Array 8000 or ESA 12000 storage subsystems, uninstall HSZdisk by selecting "Remove StorageWorks HSZdisk" and re-install HSZinstall from your RA8000 NT Platform Kit.**
8. Shutdown the system.
9. Remove the second SCSI cable path from the controller trilink.
10. Remove the terminator.
11. Reconnect the link cable between the two controllers.

The de-installation process is complete.