

COMPAQ SANworks

Secure Path Version 3.1 for Microsoft Windows

Installation and Reference Guide

Third Edition (April, 2000)
Part Number AA-RL4SC-TE
Compaq Computer Corporation

Notice

The information in this publication is subject to change without notice.

COMPAQ COMPUTER CORPORATION SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS MATERIAL. THIS INFORMATION IS PROVIDED "AS IS" AND COMPAQ COMPUTER CORPORATION DISCLAIMS ANY WARRANTIES, EXPRESS, IMPLIED OR STATUTORY AND EXPRESSLY DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR PARTICULAR PURPOSE, GOOD TITLE AND AGAINST INFRINGEMENT.

This publication contains information protected by copyright. No part of this publication may be photocopied or reproduced in any form without prior written consent from Compaq Computer Corporation.

© 2000 Compaq Computer Corporation.

All rights reserved. Printed in the U.S.A.

The software described in this guide is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of the agreement.

Compaq, Deskpro, Fastart, Compaq Insight Manager, Systempro, Systempro/LT, ProLiant, ROMPaq, QVision, SmartStart, NetFlex, QuickFind, PaqFax, ProSignia, registered United States Patent and Trademark Office.

Netelligent, Systempro/XL, SoftPaq, QuickBlank, QuickLock are trademarks and/or service marks of Compaq Computer Corporation. Neoserver is a trademark of Compaq Information Technologies Group.

Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Pentium is a registered trademark and Xeon is a trademark of Intel Corporation.

Other product names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Compaq SANworks Secure Path Version 3.1 for Microsoft Windows Installation and Reference Guide
Third Edition (April, 2000)
Part Number AA-RL4SC-TE

Contents

About This Guide

| | |
|----------------------------------|------|
| Text Conventions | vii |
| Symbols in Text | viii |
| Symbols on Equipment | viii |
| Rack Stability | ix |
| Getting Help | ix |
| Compaq Technical Support | ix |
| Compaq Website | x |
| Compaq Authorized Reseller | x |

Chapter 1

Theory of Operation

| | |
|------------------------------|-----|
| Overview..... | 1-1 |
| Features..... | 1-2 |
| Secure Path Technology | 1-2 |
| Auto-Failback..... | 1-3 |
| Path Verification..... | 1-3 |
| Load Distribution..... | 1-3 |
| Software Components..... | 1-4 |

Chapter 2

Technical Description

| | |
|--|-----|
| Overview..... | 2-1 |
| Managed Entity Profiles | 2-2 |
| Controller Ownership | 2-2 |
| Path Definition | 2-3 |
| Path Definition for Parallel SCSI-based Configurations (Windows NT only)..... | 2-3 |
| Path Definition for Fibre Channel Arbitrated Loop | 2-5 |
| Path Definition for Fibre Channel – Dual Switched Fabric..... | 2-7 |

| | |
|--|------|
| Path Status..... | 2-9 |
| Failover Operation..... | 2-10 |
| Failback Options..... | 2-11 |
| Load Distribution..... | 2-11 |
| Path Verification..... | 2-12 |
| Path Management Behavior Summary | 2-13 |

Chapter 3

Hardware Setup for Fibre Channel

| | |
|--|-----|
| Components Required for RA8000/ESA12000 (FC) Secure Path Installation..... | 3-2 |
| Installing a New RA8000/ESA12000 Secure Path Configuration..... | 3-3 |
| Adding Secure Path to an Existing RA8000/ESA12000 Configuration | 3-7 |

Chapter 4

Hardware Setup for SCSI

| | |
|---|-----|
| Secure Path (SCSI Installation) Prerequisites | 4-2 |
| RAID System Preparation..... | 4-3 |
| Preparing Existing RAID Systems for Secure Path Operation | 4-3 |
| Preparing New RAID Systems for Secure Path Operation..... | 4-3 |
| Examining the Current Single Path..... | 4-3 |
| Secure Path Installation for SCSI | 4-4 |
| Preparing and Installing SCSI HBAs..... | 4-4 |
| Cabling and Termination | 4-5 |
| Verifying the Secure Path Hardware Configuration | 4-8 |

Chapter 5

Installing Secure Path Software

| | |
|------------------------------------|-----|
| Server Software Installation | 5-2 |
| Client Software Installation | 5-3 |

Chapter 6

Managing Secure Path

| | |
|---|-----|
| Launching Secure Path Manager..... | 6-2 |
| Logging on to Secure Path Manager..... | 6-2 |
| Defining SPM Storage Profiles | 6-2 |
| Saving an SPM Storage Profile | 6-3 |
| Creating A New SPM Storage Profile | 6-4 |
| Selecting an Existing SPM Storage Profile | 6-4 |
| Editing an Existing SPM Storage Profile | 6-4 |
| Changing the Secure Path Agent Password..... | 6-4 |
| Troubleshooting Connection Problems..... | 6-5 |
| Monitoring Host Connections | 6-5 |
| Responding To A Lost Host Connection | 6-6 |

| | |
|---|------|
| Setting Storage Profile Properties..... | 6-7 |
| Storage System View..... | 6-8 |
| Physical Path View..... | 6-9 |
| Managing Storage Sets and Paths..... | 6-12 |
| Moving A Storage Set..... | 6-12 |
| Making A Path Alternate..... | 6-12 |
| Making A Preferred Path..... | 6-13 |
| Changing A Preferred Path..... | 6-13 |
| Making A Path Offline..... | 6-13 |
| Making A Path Online..... | 6-13 |
| Verifying A Path..... | 6-14 |
| Repairing A Path..... | 6-14 |
| Detecting and Identifying Path and Controller Failures..... | 6-14 |
| Detecting Path Failures..... | 6-15 |
| Identifying Path Failovers..... | 6-16 |
| Identifying Controller Failovers..... | 6-17 |
| Responding to Failover Events..... | 6-17 |
| Using SPM with MSCS and OPS Clusters..... | 6-18 |

Chapter 7

Using Secure Path with SWCC

| | |
|---|-----|
| Adding a Secure Path System to the Network..... | 7-2 |
| Using SWCC to Monitor the Secure Path System..... | 7-2 |

Chapter 8

Troubleshooting Secure Path Connection Problems

| | |
|----------------------------------|-----|
| Client/Agent Considerations..... | 8-2 |
| Network Considerations..... | 8-2 |

Appendix A

Glossary

Appendix B

Removing Secure Path Software

| | |
|------------------------------------|-----|
| Removing Secure Path Software..... | B-1 |
|------------------------------------|-----|

Appendix C

Valid ALPA Settings

Index

List of Figures

| | |
|---|------|
| Figure 2-1. Path definition in a SCSI-based Secure Path configuration..... | 2-5 |
| Figure 2-2. Path definition in a Secure Path FC-AL configuration..... | 2-6 |
| Figure 2-3. Path definition in a Secure Path Dual Cascaded Switch Fibre Channel configuration..... | 2-8 |
| Figure 4-1. Secure Path hardware interconnect – SCSI single server..... | 4-5 |
| Figure 4-2. Secure Path hardware interconnect – SCSI cluster Y-cable | 4-6 |
| Figure 4-3. Secure Path hardware interconnect – SCSI cluster hub | 4-7 |
| Figure 6-1. SPM login window with a clustered host storage profile | 6-3 |
| Figure 6-2. Host connection monitor..... | 6-5 |
| Figure 6-3. Lost host connection Icon | 6-6 |
| Figure 6-4. SPM single host storage profile – Storage System view | 6-8 |
| Figure 6-5. SPM single host storage profile – Physical Path view | 6-10 |
| Figure 6-6. Storage system path failure detected..... | 6-15 |
| Figure 6-7. Controller path failure detected | 6-15 |
| Figure 6-8. Storageset path failure detected..... | 6-16 |
| Figure 6-9. Storage system failure detected | 6-16 |
| Figure 6-10. Storage controller failure detected..... | 6-16 |
| Figure 6-11. Storageset failure detected..... | 6-16 |

List of Tables

| | |
|---|------|
| Table 2-1 Path Management Behavior Summary..... | 2-13 |
| Table 3-1 Secure Path (FC Installation) Prerequisites | 3-2 |
| Table 4-1 Secure Path (SCSI Installation) Prerequisites..... | 4-2 |
| Table 7-1 Controller Folder States | 7-3 |
| Table C-1 Valid Arbitrated Loop Physical Address (ALPA) Settings..... | C-1 |
| Table C-2 ALPA to SCSI Mapping..... | C-3 |

About This Guide

This guide is designed to be used as step-by-step instructions for installation and as a reference for operation, troubleshooting, and future upgrades.

Text Conventions

This document uses the following conventions to distinguish elements of text:

| | |
|---|---|
| Keys | Keys appear in boldface. A plus sign (+) between two keys indicates that they should be pressed simultaneously. |
| user input | User input appears in a bold typeface and in lowercase. |
| <i>FILENAMES</i> | File names appear in uppercase italics. |
| Menu Options, Command Names, Dialog Box Names | These elements appear in initial capital letters. |
| Enter | When you are instructed to <i>enter</i> information, type the information and then press the Enter key. |

Symbols in Text

These symbols may be found in the text of this guide. They have the following meanings.



WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or loss of life.



CAUTION: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.

IMPORTANT: Text set off in this manner presents clarifying information or specific instructions.

NOTE: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Symbols on Equipment

These icons may be located on equipment in areas where hazardous conditions may exist.



Any surface or area of the equipment marked with these symbols indicates the presence of electrical shock hazards. Enclosed area contains no operator serviceable parts.

WARNING: To reduce the risk of injury from electrical shock hazards, do not open this enclosure.



Any RJ-45 receptacle marked with these symbols indicates a Network Interface Connection.

WARNING: To reduce the risk of electrical shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.



Any surface or area of the equipment marked with these symbols indicates the presence of a hot surface or hot component. If this surface is contacted, the potential for injury exists.

WARNING: To reduce the risk of injury from a hot component, allow the surface to cool before touching.



Power Supplies or Systems marked with these symbols indicate the equipment is supplied by multiple sources of power.

WARNING: To reduce the risk of injury from electrical shock, remove all power cords to completely disconnect power from the system.

Rack Stability



WARNING: To reduce the risk of personal injury or damage to the equipment, be sure that:

- The leveling jacks are extended to the floor.
 - The full weight of the rack rests on the leveling jacks.
 - The stabilizing feet are attached to the rack if it is a single rack installations.
 - The racks are coupled together in multiple rack installations.
 - A rack may become unstable if more than one component is extended for any reason. Extend only one component at a time.
-

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 Technical Support

You are entitled to free hardware technical telephone support for your product for as long you own the product. A technical support specialist will help you diagnose the problem or guide you to the next step in the warranty process.

In North America, call the Compaq Technical Phone Support Center at 1-800-OK-COMPAQ. This service is available 24 hours a day, 7 days a week. For continuous quality improvement, calls may be recorded or monitored.

Outside North America, call the nearest Compaq Technical Support Phone Center. Telephone numbers for world wide Technical Support Centers are listed on the Compaq website. Access the Compaq website at <http://www.compaq.com>.

Be sure to have the following information available before you call Compaq:

- Technical support registration number (if applicable)
- Product serial number (s)
- Product model name(s) and numbers(s)
- Applicable error messages
- Add-on boards or hardware
- Third-party hardware or software
- Operating system type and revision level

Compaq Website

The Compaq website has information on this product as well as the latest drivers and Flash ROM images. You can access the Compaq website at <http://www.compaq.com>

Compaq Authorized Reseller

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.
- Elsewhere, see the Compaq website for locations and telephone numbers.

Chapter 1

Theory of Operation

Overview

Compaq SANworks Secure Path for Microsoft Windows is a high-availability software product that manages and maintains continuous data access to the following Compaq StorageWorks storage systems:

- StorageWorks Ultra SCSI RAID Array 7000 / Enterprise Storage Array 10000 (Windows NT 4.0 only)
- StorageWorks Fibre Channel RAID Array 8000 / Enterprise Storage Array 12000 (Windows NT 4.0 or Windows 2000)

You can use this software with StorageWorks RAID Arrays configured to operate on Intel-based platforms running Windows NT 4.0 or Windows 2000 operating systems in single host server, Microsoft Cluster Server (MSCS), and Oracle Parallel Server (OPS) high-availability environments.

Secure Path eliminates the disk drive, RAID controller, host bus adapter (HBA), and interconnect hardware (cables, hubs or switches, and connectivity devices) as single points of failure in the storage system.

Through the deployment of redundant hardware and advanced RAID technology, Secure Path enhances fault tolerance and storage system availability by providing automated failover capability.

Redundant physical connections define separate physical “paths” in a Secure Path hardware configuration. Each path originates at a unique HBA port on the server, and ends at a unique RAID controller port in the storage system.

Features

Secure Path provides the following features:

- Allows StorageWorks dual-controller RAID systems and host servers equipped with multiple HBAs redundant physical connectivity along independent SCSI, Fibre Channel Arbitrated Loop (FC-AL) or Fibre Channel switched fabric paths.
- Monitors each path and automatically re-routes I/O to a functioning alternate path if an HBA, cable, hub, switch or controller failure occur.
- Determines the “health” of available storage units and physical paths through the implementation of path verification diagnostics.
- Monitors and identifies failed paths and failed-over storage units.
- Facilitates static load balancing, which allows manual movement of devices between paths.
- Automatically restores failed-over storage units to repaired paths with auto-failback capability enabled.
- Implements anti-thrash filters to prevent failover/failback effects caused by marginal or intermittent conditions.
- Exploits the potential for improved data throughput and increased bandwidth using dual RAID controllers configured in multiple-bus mode operation with load distribution capability enabled.
- Detects failures reliably without inducing false or unnecessary failovers.
- Implements failover/failback actions transparently without disrupting applications.
- Provides Client/Server remote management capability, and multiple storage system support.

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 multiple-bus mode. Multiple-bus mode allows each controller to process I/O independently of the other controller 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 is used for access at system boot time. During runtime, storage units may be moved between paths at any time through use of the

Secure Path Management utility. On HSG80 RAID devices, storage units may also be accessed on each controller through either of two available ports.

The Secure Path software detects the failure of I/O operations on a failed path and automatically re-routes traffic to other available paths. Secure Path software will seek alternate paths through available SCSI buses, Fibre Channel hubs or switches, controllers, controller ports, and/or host bus adapters. Path failover is completed seamlessly, without process disruption or data loss.

Following a warm-swap of an adapter or cable component, failed controller, hub, or switch, 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 MSCS configurations.

Auto-Failback

With auto-failback enabled, Secure Path monitors failed paths and automatically returns failed-over storage units to their original path once the path has been restored. Anti-thrash filters prevent “ping pong” effects (repeated failover/failback operations) caused by marginal or intermittent conditions. The user may select auto or manual failback policy using the Secure Path Management utility.

Path Verification

Path verification implements diagnostics that periodically determine the health of available storage unit paths. Path verification ensures that path status is both accurate and current. Through this background testing of active and available paths, problems may be detected and corrected, ensuring path integrity.

Load Distribution

Secure Path takes advantage of the potential of multiple path access and enhances I/O performance through use of load distribution capability. With this feature enabled, Secure Path evenly distributes I/O operations across all available paths to a given storage unit.

Software Components

The Secure Path Software Kit for Windows includes the following software components:

- **HszDisk.sys** is a Windows NT class driver that provides unique error handling features and performance enhancements unavailable in the native Windows NT disk class driver. It 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 recovery operations.
- **RaiDisk.sys** is a Windows filter driver that provides the primary failover capability in the Secure Path product. RaiDisk supports StorageWorks RAID Array multiple-bus mode, multiple path access, and provides all functions required for monitoring I/O and detecting path failures. In Windows 2000 applications, RaiDisk also transparently integrates the functionality that HszDisk does for Windows NT.
- **Secure Path Manager** is the client/server application used to manage multiple path StorageWorks RAID Array configurations. It displays a graphical representation of multiple path environments, indicating status of all configured storage units and paths. It runs locally at the managed servers, or remotely at a management workstation.

To facilitate static load balancing, Secure Path Manager provides the capability to move storagesets between paths. It indicates which path is currently servicing each configured storage unit, and displays the mode and state information for all available paths.

- **Secure Path Agent** is a Windows service that communicates with the RaiDisk filter driver on the host server, and Secure Path Manager on the client side, using the TCP/IP protocol and WinSock API. It installs on the host server along with the RaiDisk driver.

To minimize network traffic, display information is relayed from the Secure Path Agent to the Secure Path Manager only when the RaiDisk driver detects changes in the configuration. The Secure Path Agent also notifies StorageWorks Command Console (SWCC) clients when RaiDisk performs path failover or auto-failback operations.

- **Secure Path Setup** supports driver and application installation and de-installation with Windows NT 4.0 and Windows 2000.

Each software component of Secure Path makes use of the Windows Event Log to post error and informational messages as required.

Chapter 2

Technical Description

Overview

Compaq SANworks Secure Path is a server-based software product that enhances StorageWorks RAID Array storage systems by providing automatic recovery from server-to-storage system connection failures. Secure Path supports multiple I/O paths between host and storage, improving overall data availability. If any component in the path between host and storage fails, Secure Path redirects pending and subsequent I/O requests to an alternate path.

This chapter provides technical details on the following Secure Path subjects:

- Reference material for managed entity profiles
- Controller ownership requirements
- Path definition details
- Failover operations and options
- Path management behavior summary

Managed Entity Profiles

You can manage large configurations through a single instance of the Secure Path Manager. However, there are certain practical limits on the configuration size that can be displayed and managed in a single graphical window. Secure Path Manager uses the concept of the “managed entity” or “profile” to express this working configuration limit.

The profile limits for Secure Path Manager are a maximum of 8 servers (host systems) connected to and sharing up to 8 storage systems, configured for multiple-bus failover mode. The host servers may be standalone servers or grouped into clusters. All servers in the profile must have access to all of the storage systems listed in that profile.

Secure Path does not provide any mechanism for synchronizing access to or guaranteeing the data integrity of storagesets shared across multiple standalone hosts or clusters. Access to storagesets must be restricted to a single standalone server or a single “clustered” host set.

The Secure Path Manager lets you create multiple profiles stored as separate files in the same directory. Any given server, cluster or storage system may exist in multiple profiles as long as the profile configuration rules described above are followed.

Controller Ownership

Storage systems that are multiple-bus capable generally contain a pair of redundant controllers and support one of the following basic operational models:

- active/passive
- active/active

In the active/passive model, all storagesets are assigned to one of the controller pair for I/O processing with the other controller inactive, but available as a substitute in case of failure on the original.

In the active/active model, I/O may be routed through both controllers simultaneously, providing better performance in addition to high availability.

The RA7000/8000 and ESA10000/12000 RAID Arrays supported by Secure Path implement a modified version of the active/active model. While I/O can be processed simultaneously by both controllers, any given storageset is “owned” or online to a host through only one controller. Ownership of a

storage set may be transferred to the other controller at any time through a host-initiated command sequence.

However, since the ownership transfer results in controller cache flushing and I/O wind down, the storage set may become inaccessible for a period of several seconds to complete this sequence. Arbitrary ownership transfers should be avoided by the user, and are never automatically initiated by Secure Path.

NOTE: Secure Path automatically retries I/O requests that terminated in error due to ownership transfers. It also queues new I/O requests until the ownership transfer has completed to insure data integrity.

Path Definition

Within Secure Path, a path is defined as the collection of physical interconnect components including HBAs, switches or hubs, cables, RAID array controllers and the ports on the controllers. Since the Secure Path filter driver component, RaiDisk, positions itself between the port and class driver layers of Windows, it can only distinguish physical paths when elements of the SCSI equivalent address are different.

Some configurations include multiple cascaded switches within a fabric with the switches connected by one or more inter-switch links. These paths are neither directly visible to nor manageable by Secure Path. While these inter-switch paths provide an additional level of redundancy within the fabric, their management is handled directly within the switch. Refer to the documentation received with your switch hardware for more information about inter-switch link routing and failover policies.

Path Definition for Parallel SCSI-based Configurations (Windows NT only)

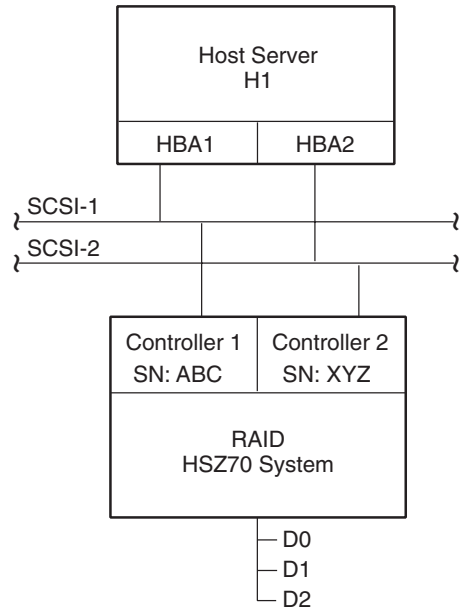
In parallel SCSI configurations, a path consists of the complete physical interconnection from a given host to a specific storage set in a RAID storage system. In Windows NT 4.0, there are four parts of an address that define a given path to a specific storage set.

- **Port number** is created by Windows and refers to a specific SCSI adapter. Numbers are zero-based and assigned in the order of discovery, hence they are relative and may change as a result of system reconfigurations such as adding or removing other SCSI adapters. Secure Path Manager displays the port number in the column headed “HBA” as shown in Figure 2-1.
- **Bus number** is a value resulting from the design of the SCSI adapter itself and refers to the number of physically independent interconnects supported; this number is currently always zero for SCSI adapters running with Secure Path.
- **Target ID and LUN** are values which are set in the RAID Array controller in the unit name, in the form “Dxxy” in which ‘xx’ is the target number (0 – 15) and ‘yy’ is the LUN (0 – 7 for Windows).

NOTE: If the target number is 0, it is dropped from the unit number designation, so the unit number D0 is understood to be LUN 0 on target 0 while D100 is LUN 0 on target 1. Every storageset configured on an RA7000 or ESA10000 must have a unique unit name assigned to it.

There are generally no more than two SCSI paths from a host to a specific LUN. The path addressing under Windows is adapted directly from SCSI-defined addresses and each path implies connection to a discreet controller. Since the RA7000 and ESA10000 present an identical address space from both controllers, the port number is the only

bit of address information which will be different across the paths from a given host to a specific storage set.



SHR-1569

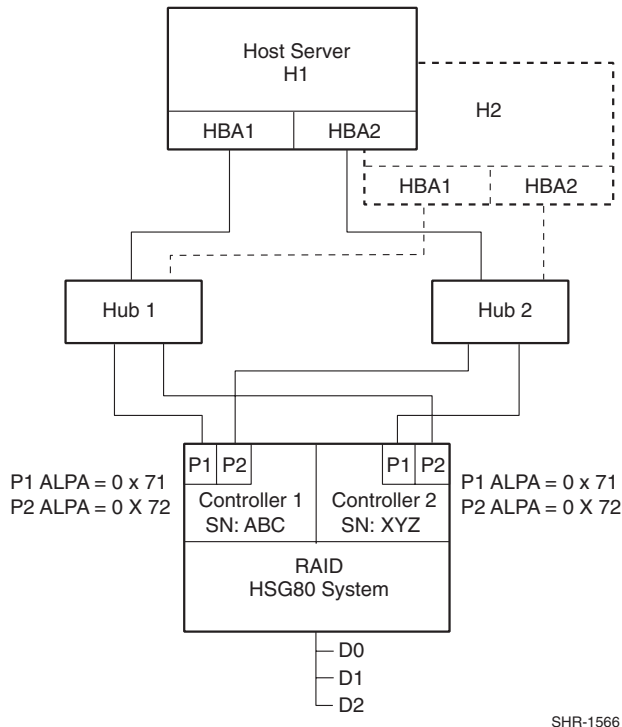
| | Host | Controller Serial No. | Host Bus Adapter | Bus-Target-LUN |
|------------------|------|-----------------------|------------------|----------------|
| Drive D: (D1) | H1 | ABC | 1 | 0-0-1 |
| | H1 | XYZ | 2 | 0-0-1 |

Figure 2-1. Path definition in a SCSI-based Secure Path configuration

Path Definition for Fibre Channel Arbitrated Loop

In FC-AL configurations, devices are accessed within Windows NT 4.0 and Windows 2000 using conventional SCSI addressing terminology. Fibre Channel adapters are referred to as HBAs, which are named and numbered as SCSI ports. The rest of the SCSI address, except for the LUN, is created within the Fibre Channel's mini-port driver and is derived from the ALPA (Arbitrated Loop Physical Address) assigned to each port on the RA8000/ESA12000 controllers.

The LUN number is derived from the unit number assigned to the storageset within the controller using SWCC or CLI commands. Each connected node on an arbitrated loop must have a unique ALPA assigned.



SHR-1566

| | Host | Controller Serial No. | Host Bus Adapter | Bus-Target-LUN |
|------------------|------|-----------------------|------------------|----------------|
| Drive D: (D1) | H1 | ABC | 1 | 3-3-1 |
| | H1 | XYZ | 1 | 3-2-1 |
| | H1 | XYZ | 2 | 3-3-1 |
| | H1 | ABC | 2 | 3-2-1 |
| | H2 | ABC | 1 | 3-3-1 |
| | H2 | XYZ | 1 | 3-2-1 |
| | H2 | XYZ | 2 | 3-3-1 |
| | H2 | ABC | 2 | 3-2-1 |

Figure 2-2. Path definition in a Secure Path FC-AL configuration

In Figure 2-2, Hub 1; Controller 1, Port 1 (C1-P1; ALPA = 0x71) and Controller 2, Port 2 (C2-P2; ALPA = 0x72) constitute one arbitrated loop. Hub

2, Controller 1, Port 2 (C1-P2; ALPA =0x72) and Controller 2, Port 1 (C2-P1; ALPA = 0x71) constitute a second loop.

The LP6NDS35 mini-port driver for the KGPSA Fibre Channel adapter uses a fixed mapping scheme to translate ALPA assignments to SCSI bus and target ID values. Appendix C provides a complete listing of KGPSA ALPA to SCSI mapping.

When installed in your system, the adapter is instructed to perform scan-down, starting from the highest ALPA and moving downward. The adapter maps ALPA 0x71 to Bus 3, Target ID 3.

NOTE: Even though the KGPSA has only a single physical Fibre Channel interconnect, it artificially expands the enumeration of buses to allow mapping of the supported Fibre Channel ALPA address space into the Windows SCSI address space. Bus 0 is never used and we recommend that ALPAs below 0x71 be reserved for adapter assignments.

In most configurations, the same ALPAs are assigned to the respective ports of the two RA8000/ESA12000 controllers. Since the ALPA to SCSI address mapping is fixed, this results in identical SCSI B-T-L values for the pair of P1 ports and the pair of P2 ports. The controller serial number information in the display provides a mechanism to correlate path information to a specific controller for maintenance purposes.

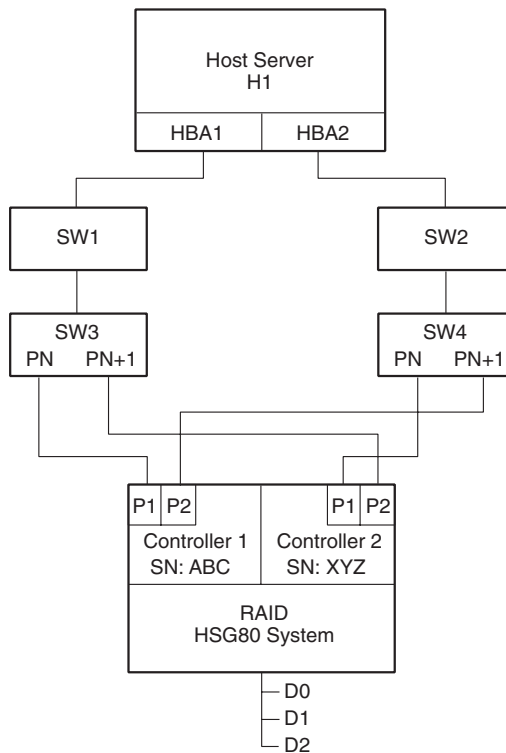
NOTE: In FC-AL topology, knowing the ALPA assignment for a particular controller port, allows explicit path resolution to the port level.

Figure 2-2 also shows how the Secure Path Manager displays path information in the event that multiple hosts have access to the same device, as would occur in an MSCS environment.

Path Definition for Fibre Channel –Dual Switched Fabric

Figure 2-3 depicts a dual cascaded switch Fibre Channel topology and the resulting path connection information displayed by Secure Path Manager. Fibre Channel adapters are referred to as HBAs and are named and numbered by Windows as SCSI ports. The rest of the SCSI address, except for the LUN, is created through the Fibre Channel mini-port driver. It is derived ultimately from Fibre Channel addressing information, which is influenced by connections between the controller, and the switch domain and port number.

The LUN corresponds directly to the Unit Number assigned to the storageset through SWCC or CLI command.



SHR-1567

| | Host | Controller Serial No. | Host Bus Adapter | Bus-Target-LUN |
|------------------|------|-----------------------|------------------|----------------|
| Drive D: (D1) | H1 | ABC | 1 | 1-0-1 |
| | H1 | XYZ | 1 | 1-1-1 |
| | H1 | XYZ | 2 | 1-0-1 |
| | H1 | ABC | 2 | 1-1-1 |

Figure 2-3. Path definition in a Secure Path Dual Cascaded Switch Fibre Channel configuration

In Figure 2-3, devices found on SW3-Pn are assigned the first available bus/target numbers: 1 and 0, respectively.

NOTE: KGPSA mini-port driver LP6NDS35 normally reserves Bus 0.

The LUN number is derived from the unit number assigned to the storageset within the controller using SWCC or CLI commands. The next port, SW3-Pn+1, gets the next sequential value of 1 – 1. If there were additional storage systems connected, the address mapping would continue incrementing Target numbers up to 31, at which point Bus 2 Target 0 would be assigned.

Because the two independent fabric connections in Figure 2-3 are symmetrical (the lower switch port number is connected to the lower controller port number), the address mapping for the second fabric is identical to the first. The HBA number is the only exception. Although not required for correct operation of Secure Path, symmetric cabling is strongly recommended in Fabric topologies. By following this cabling convention, the controller port number corresponding to a given path in the Secure Path Manager is implied.

Path Status

Secure Path displays Path Status using Path Mode and Path State attributes.

Path Mode may be one of Preferred, Alternate, and Preferred-Offline (pre-offline) or Alternate-Offline (alt-offline).

- **Preferred Path Mode** indicates the user-specified path that will be used to communicate from a specific host to the specified storageset. With Load Distribution disabled at system boot, RaiDisk declares the first path discovered as the Preferred path on the owning controller. With Load Distribution enabled, RaiDisk declares **all** paths on the owning controller Preferred. The user may modify the default driver's path settings using Secure Path Manager.
- **Alternate Path Mode** indicates those that are not user-preferred. These paths provide the redundancy in case preferred paths fail.
- **Offline Path Modes** (Preferred-Offline or Alternate-Offline) include the original mode (via the prefix) and indicate the user has specified the path should never be used for I/O. Paths are marked offline only as a result of user specification.

Path State may be Active, Available, or Failed. State is set automatically by RaiDisk and reflects current actual path status, which may deviate from user expectations because of path failures.

- **Active State** indicates the associated path is currently servicing, or is capable of servicing I/O to the storageset. When Load Distribution is enabled, multiple paths from a common host to storageset may be in the Active State.

- **Available State** indicates the associated path belongs to the set of redundant paths to the storage set that could be utilized during failover.
- **Failed State** indicates the path has encountered errors either during normal operation or as a result of Path Verification testing.

Chapter 6, “Managing Secure Path,” provides a more detailed discussion of Path Modes and Path States, and provides illustrative examples of the effects of failover, failback, and user intervention.

Failover Operation

Failover occurs automatically when a selected set of error conditions is detected. Secure Path normally performs path failover only when user I/O is active. However, it is possible for Secure Path Manager to show some units with a common failed path in the failed over state while other units appear to remain accessible through that path.

Failover follows a certain hierarchy, conditioned by the state of Load Distribution. Secure Path does not change the mode of “Preferred” or “Alternate” paths in failover situations, so you can restore original path assignments after making repairs.

- **Load Distribution *disabled*:**

Secure Path marks the “Preferred-Active” path failed and switches to the next “Alternate – Available” path connected to the same controller, if such exists.

If there is no “Alternate – Available” path on the same controller, Secure Path attempts to move the device to an “Alternate – Available” path on the other controller. Secure Path changes individual “Alternate-Available” paths to “Alternate-Active” in accordance with its default path assignment algorithm.

- **Load Distribution *enabled*:**

Initially, failover consists of marking a bad path “failed,” which effectively removes it from the list of usable paths for the storage set.

If no “Preferred – Active” paths remain for the device, Secure Path activates an “Alternate – Available” path on the same controller, if one exists.

If no “Alternate – Available” paths remain on the same controller Secure Path attempts to move the device to an “Alternate – Available” path on the other controller. Additionally, Secure Path sets all “Alternate-Available” paths to “Alternate-Active.”

Failover policy is optimized to minimize performance impact to the overall configuration. Load Distribution is the only parameter the user can set in Secure Path failover policy

Table 2-1 provides a summary chart of path management behavior, conditioned by the several optional features of Secure Path.

Failback Options

Secure Path allows manual or automatic path failback. In manual mode, devices are restored to their original path either through drag-and-drop operation (controller failback) or action menu items (Repair). The operation is performed regardless of whether there is system I/O in process to the selected device.

When set to automatic mode, Secure Path tests a failed path at fixed intervals if I/O is in process for the affected device. If the path appears to be viable, the Path State is set to Active and I/O will again be routed through this path.

Secure Path implements an anti-thrash filter to avoid indefinitely moving a device back and forth in the presence of an intermittent failure mode. If, within a given period of time (currently one hour), Secure Path detects that a device has failed back twice, and the original path again causes a failover, the device will be left on the failed over path for the duration of the timer interval. At the end of the timer interval, the anti-thrash filter is re-initialized and the failover/failback process repeats if the intermittent failure cause persists.

Load Distribution

When enabled, Load Distribution allows multiple paths between a host and a specific storage set to be utilized in parallel. Fibre Channel interconnection schemes result in multiple paths between a host and each controller. I/O intended for storage sets connected to a given controller, alternately dispatch through the set of appropriate paths, spreading the load across all components in the RAID storage system and maximizing performance potential. Load Distribution may not be used in Microsoft Clusters or other environments that utilize device reservations as a lock mechanism since the RAID Array controllers in RA8000/ESA12000 enforce reservations on a per-port basis.

Load Distribution requires a Fibre Channel configuration that results in at least four unique paths from the host node to the storage system. While this can be accomplished with several different physical configurations, maximum performance potential is achieved when all four ports of the RAID storage system are used. Since the RA7000/ESA10000 have only one port per controller they do not normally benefit from Load Distribution.

When Load Distribution is enabled, the Secure Path driver causes all paths to the owning controller to be marked “Preferred” by default. This is true when a host boots up, when Secure Path fails over a storageset from one controller to the other, or when a user manually moves a selected storageset between controllers using Secure Path Manager. The user may also modify the operational mode of individual paths to discrete storagesets using the Manager.

Path Verification

When enabled, Path Verification causes Secure Path to periodically test the viability of all paths to all storagesets for paths marked “Available,” “Failed,” or “Active.” However, Path Verification does not test paths that are in an “offline” mode.

Path Verification is useful for detecting failures that affect overall path redundancy before they affect failover capability. If a “Preferred” path fails path verification, failover occurs. If an “Alternate” path fails path verification, its state will change from “Available” to “Failed.”

If a path marked “Failed” passes path verification, the Path State is set to “Available.” If auto-failback is enabled, the “Preferred” path becomes “Active.”

Path Management Behavior Summary

Reference the chart in Table 2-1 for a summary of path management behavior conditioned by the optional features of Secure Path.

**Table 2-1
Path Management Behavior Summary**

| | | |
|----------------------------|--|--|
| No I/O Distribution | Startup | <ol style="list-style-type: none"> 1) Choose first path to controller on which LUN is online as preferred active, port does not matter – all other paths on both controllers marked alternate available. 2) If no online path is found, make any available path online and use as preferred active – all other paths marked alternate available |
| | Active Path Failure | <ol style="list-style-type: none"> 1) Path marked preferred (or alternate) failed and fails to any other alternate available path on same controller, then other controller – port does not matter. Alternate available path used is marked alternate active. 2) Behavior is the same with I/O or background path verification. 3) If LUN reserved, mark paths failed, but do not fail to other path on non-owning node. |
| | Available Path Failure Path verification | <ol style="list-style-type: none"> 1) Failed path marked failed. 2) Behavior is result of background path verification. |
| | Path Repaired | <ol style="list-style-type: none"> 1) Path marked available 2) If autofailback is enabled, failback to preferred path from available path as regular “autofailback” function. 3) If LUNs reserved, mark path available but do not autofailback on non-owning node. |

continued

Table 2-1
Path Management Behavior Summary *continued*

| | | |
|---|--|--|
| With I/O Distribution (LUN reservation not supported) | Startup | 1) Choose all paths to controller on which LUN is online as preferred active , port does not matter – all paths to other controller marked alternate available . 2) If no online path is found, make any available path online and use as preferred active – all other paths marked alternate available . |
| | Active Path Failure | 1) Path marked (preferred or alternate) failed . 2) If path is preferred active , change to alternate available on same controller, then other controller. 3) Behavior is the same with I/O or background path verification. |
| | Available Path Failure Path Verification | 1) Path marked failed . 2) Behavior is result of background path verification. |
| | Path Repaired | 1) Path marked available 2) Path made active if preferred , and other preferred paths are active. 3) If autofailback is enabled, failback to preferred paths from available as regular “autofailback” function. |

Chapter **3**

Hardware Setup for Fibre Channel

This chapter provides the following Secure Path Fibre Channel hardware setup information:

- Reference material for high-availability connection options
- Installation prerequisites
- Installation procedures for new Secure Path Fibre Channel configurations
- Installation procedures for building Secure Path into existing Fibre Channel configurations

Before installing Secure Path on a new or existing Fibre Channel (FC) configuration, first review the RA8000/ESA12000 High Availability Application Notes found on the Compaq web site. They will familiarize you with various high-availability connection layouts for FC devices and cabling.

The Application Notes present a topological layout of several high-availability options. They also list part numbers, related reference documentation, and discuss restrictions that apply when Secure Path co-exists with MSCS software and FC hardware devices.

The High-Availability Application Notes for FC installations are:

| | |
|---|-------------|
| RA8000/ESA12000 FC-AL High Availability Configurations for Windows NT – Intel | AA-RH0SC-TE |
| RA8000/ESA12000 FC-Switch High Availability Configurations for Windows NT – Intel | AA-RHH6C-TE |

NOTE: For the most current Application Notes, visit the Compaq website at: www.compaq.com/products/storageworks.

Components Required for RA8000/ESA12000 (FC) Secure Path Installation

Verify receipt of the Secure Path software kit and the FC hardware ordered for the installation. If you are missing any component, please contact the account representative or call the Compaq Customer Services Hotline at (800) 354-9000. The basic requirements for Secure Path operation are listed in Table 3-1.

**Table 3-1
Secure Path (FC Installation) Prerequisites**

| Host Feature | Requirement |
|--------------------------|--|
| Platform | Intel |
| Operating System | Windows NT Enterprise Edition, Version 4.0 Windows 2000 Advanced Server Edition |
| Secure Path Software Kit | SANworks Secure Path v3.1 Enterprise Edition for Microsoft Windows (QB-669AD-SA) |
| RAID Storage System(s) | StorageWorks dual-redundant RA8000/ ESA12000 (FC) |
| Solution Software Kit | StorageWorks Solution Software V8.5 for Windows NT (QB-65RAE-SA) |

continued

Table 3-1
Secure Path (FC Installation) Prerequisites *continued*

| Host Feature | Requirement |
|---|--|
| StorageWorks Command Console | Storage management software |
| Host Bus Adapter(s) (and adapter driver) | Supported model for Windows NT - Intel: StorageWorks KGPSA |
| FC Interconnect Hardware | FC hubs, switches, and connection hardware as required (Application Notes provide detailed equipment part numbers) |
| Service Tools | Appropriate tools to service the equipment |
| Technical Documentation | The reference guides for the RAID system, the host server and the Microsoft Windows software |

Installing a New RA8000/ESA12000 Secure Path Configuration

This section provides procedures to install and configure a Secure Path topology for *new* FC hardware installation.

1. Install all of the new RAID storage system and FC interconnect hardware (hubs/switches) and cabling according to the instructions provided with the installation documentation shipped with the FC equipment.
2. Establish a serial link to the RAID system. You may use a serial line connection from the host server or from any PC workstation. Obtain RAID controller status using the StorageWorks Command Console (SWCC) Command Line Interface (CLI) or a terminal emulation program, such as HyperTerminal.
3. Using the CLI, complete the following steps to configure the RAID system for Secure Path operation. For FC-AL configurations, perform step a. For FC Switched Fabric configurations, perform step b. For either, continue with step c.
 - a. For FC-AL configurations, set the Arbitrated Loop Physical Address (ALPA) for HSG80 controllers in the RAID system using the following commands:

```
HSG80> set this_controller port_1_topology=offline
```

```
HSG80> set other_controller port_1_topology=offline
```

```
HSG80> set this_controller port_1_al_pa=n+1
```

```
HSG80> set other_controller port_1_al_pa=n+1
```

Where n+1 is an available ALPA address selected from the table in Appendix C.

```
HSG80> set this_controller port_1_topology=loop_hard
```

```
HSG80> set other_controller port_1_topology=loop_hard
```

```
HSG80> set this_controller port_2_topology=offline
```

```
HSG80>set other_controller port_2_topology=offline
```

```
HSG80> set this_controller port_2_al_pa=n
```

```
HSG80> set other_controller port_2_al_pa=n
```

Where n is an available ALPA address selected from the table in Appendix C

```
HSG80> set this_controller port_2_topology=loop_hard
```

```
HSG80>set other_controller port_2_topology=loop_hard
```

- b. For FC Switched Fabric configurations, use the following commands:

```
HSG80> set this_controller port_1_topology=fabric
```

```
HSG80> set other_controller port_1_topology=fabric
```

```
HSG80> set this_controller port_2_topology=fabric
```

```
HSG80>set other_controller port_2_topology=fabric
```

- c. Configure the RAID system controllers for multiple-bus failover mode using the commands below.

```
HSG80 > set nofailover
```

IMPORTANT: The “other” controller will shutdown and must be manually restarted by momentarily depressing the reset button on the controller’s front panel. Wait for two minutes for the controller to boot before proceeding.

```
HSG80 > set multibus copy=this
```

The controllers will restart in multiple-bus mode.

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

```
HSG80 > show this
```


Verify that the data returned to this command includes the statement that the controller is in a multiple-bus dual redundant configuration.

The controllers are now configured for multiple-bus operation.

4. Install all Windows servers and all HBAs. Referencing Chapter 1 of the *RAID Solution Software for Windows– Installation Reference Guide*, run the FC software setup (included with the RA8000/ESA12000 platform kit) on the host server(s) to set HBA parameters.

IMPORTANT: Do not connect HBAs to any switches/hubs at this time.

5. Install Secure Path software on the Windows server(s).
The Secure Path software is installed using the Secure Path setup wizard. To launch the Secure Path installation wizard, insert the *SANworks Secure Path Software v3.1 for Microsoft Windows* CD into the CD-ROM driver. Please refer to Chapter 5, “Installing Secure Path Software,” to complete the Secure Path software installation setup.
6. Shut down the server(s).
7. Connect all HBAs to the switches/hubs.
8. Restart the server(s) one at a time, performing each step below. Repeat this step until all servers have been brought online.
 - a. Using SWCC double-click on the desired controller icon in the main window. Choose the Connection tab to rename connections. Suggested connection names are listed in the Application Notes. Refer to the SWCC documentation if you need more information about managing connections.
 - b. Set Unit Offsets so that each server or cluster requiring exclusive access to a set of LUNs has its own unique offset range. Each connection is restricted to a maximum of 8 LUNs.
 - c. Create storage sets and provide unit attributes for LUNs on this server or cluster, including Preferred Path assignments using SWCC.

NOTE: Unit Number assignments must be made based on the Unit Offset numbers created in step 8b, and should be consecutive from the base offset number.

- d. Set Access IDs for each LUN to selectively present it to the appropriate standalone server or clustered servers.

9. Shut down the controllers in all RAID Array cabinets. Refer to RA8000/ESA 12000 documentation for any timing restrictions that may apply to storageset creation and controller shutdown. Shut down all servers and turn off power. Power-cycle all RAID Array storage systems. If the RAID Array cabinet contains redundant power supplies, be sure to power cycle them simultaneously.
10. Restart all servers and verify the configuration.

Following system reboot, check the Windows system event log for successful start events for the RaiDisk, and HszDisk (for Windows NT 4.0 only) drivers.

Check the Windows application event log for a successful start event for the Secure Path Agent.

You have now completed the configuration procedures required to support the new Secure Path environment. See Chapter 6, "Managing Secure Path," for information on monitoring and managing Secure Path activity using the Secure Path Manager.

Adding Secure Path to an Existing RA8000/ESA12000 Configuration

This section assumes that a single FC path exists between an RA8000 or ESA12000 system and host server.



WARNING: For each RAID system in a production environment being converted to Secure Path operation, make sure that all users have logged off the Windows server(s) and that all I/O to the RAID system(s) has ceased. Follow normal procedures to backup the storage systems before proceeding.

1. Using the CLI, complete the following steps to configure the RAID system for Secure Path operation:
 - a. Configure the RAID system controllers for multiple-bus failover mode, using the following command:

```
HSG80 > set nofailover
```

IMPORTANT: The “other” controller will shutdown and must be manually restarted by momentarily depressing the reset button on the controller’s front panel. Wait for two minutes for the controller to boot before proceeding.

```
HSG80 > set multibus copy=this
```

The controllers restart in multiple-bus mode.

After the other controller has restarted, verify that both controllers are configured for multiple-bus mode by issuing the following command:

```
HSG80 > show this
```

Verify that the data returned to this command includes the statement that the controller is in a multiple-bus, dual redundant configuration.

The controllers are now configured for multiple-bus operation.

- b. Specify the preferred controller assignment for each storage unit in the configuration, using the following commands:

NOTES:

- Secure Path configurations using all four controller ports for path redundancy are limited to a maximum of 8 LUNs.
- It is recommended that, initially, that storagesets be balanced across the controllers. As storage demands are defined, and individual drive throughput requirements are understood, adjustments to the disk I/O path configuration can be made using the StorageWorks Secure Path Manager, as described in Chapter 6.

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

```
HSG80 > show units
```

Use the following commands to specify preferred_path for units:

```
HSG80 > set (unit #) preferred=this
```

- or -

```
HSG80 > set (unit #) preferred=other
```

- c. Cycle power on the RAID cabinet for the preferred path settings to take effect.
2. Using the CLI, complete the following steps to configure the RAID system for Secure Path operation. For FC-AL configurations perform step a. For FC Switched Fabric configurations perform step b.
- a. For FC-AL configurations, if the configuration entails utilizing additional ports on existing RAID system controllers, or if you are installing additional (new) RAID systems, use SWCC to establish the Arbitrated Loop Physical Address (ALPA) assignments for all new controller ports by typing the following commands:

```
HSG80> set this_controller port_1_topology=offline
```

```
HSG80> set other_controller port_1_topology=offline
```

```
HSG80> set this_controller port_1_al_pa=n+1
```

```
HSG80> set other_controller port_1_al_pa=n+1
```

Where n+1 is an available ALPA address selected from the table in Appendix C.

```
HSG80> set this_controller port_1_topology=loop_hard
```

```
HSG80> set other_controller port_1_topology=loop_hard
```

```
HSG80> set this_controller port_2_topology=offline
```

```
HSG80>set other_controller port_2_topology=offline
```

HSG80> **set this_controller port_2_al_pa=n**

HSG80> **set other_controller port_2_al_pa=n**

Where *n* is an available ALPA address selected from the table in Appendix C.

HSG80> **set this_controller port_2_topology=loop_hard**

HSG80>**set other_controller port_2_topology=loop_hard**

- b. For FC Switched Fabric environments enter the following commands:

HSG80> **set this_controller port_1_topology=fabric**

HSG80> **set other_controller port_1_topology=fabric**

HSG80> **set this_controller port_2_topology=fabric**

HSG80>**set other_controller port_2_topology=fabric**

3. Shut down the server(s).
4. Install all FC interconnect hardware, including additional HBAs required to establish additional path(s) necessary to configure the desired High Availability topology. Reference the installation guides provided with the FC equipment for assistance.

NOTE: Do not connect new HBAs to the hubs/switches at this time.

5. Restart the server(s).
6. Referencing Chapter 1 of the *Compaq StorageWorks RAID Solution Software for Windows Installation Reference Guide*, run the FC software setup (included with the RA8000/ESA12000 platform kit) on the host server(s) to set HBA parameters.
7. Install Secure Path software on the Windows server(s).
The Secure Path software is installed using the Secure Path setup wizard. To launch the Secure Path installation wizard, insert the SANworks Secure Path Software v3.1 for Microsoft Windows CD into the CD-ROM drive. See Chapter 5, "Installing Secure Path Software," to complete the Secure Path software installation setup. If no additional paths to the storagesets are being added at this time, you should skip to step 9.
8. Restart the server(s) one at a time, performing each step below. Repeat this step until all servers have been brought online.

- a) Using SWCC, double-click the desired controller icon in the main window. Choose the Connection tab to rename connections. Suggested connection names can be found in the Application Notes. Refer to the SWCC documentation if you need more information about managing connections.
 - b) Set Unit Offsets so that each server or cluster requiring exclusive access to a set of LUNs has its own unique offset range. Each connection is restricted to a maximum of 8 LUNs.
 - c) Create any additional storagesets and/or modify unit attributes for LUNs on this server or cluster, including Preferred Path assignments using SWCC. Unit Number assignments must be made based on the Unit Offset numbers created in step 8b, and should be consecutive from the base offset number.
 - d) Set Access IDs for each LUN to selectively present it to the appropriate standalone server or clustered servers.
9. Restart the server(s).
10. Verify the Secure Path configuration.

Following system reboot, check the Windows system event log for successful start events for the RaiDisk, and HszDisk (for Windows NT 4.0 only) drivers.

Check the Windows application event log for a successful start event for the Secure Path Agent.

You have now completed the configuration procedures required to support the new Secure Path environment. See Chapter 6, "Managing Secure Path," for information on monitoring and managing Secure Path activity using the Secure Path Manager.

Chapter 4

Hardware Setup for SCSI

This chapter provides the following Secure Path SCSI hardware setup information:

- Installation prerequisites
- Preparing your RAID system for Secure Path operation
- Installation procedures for SCSI configurations

This chapter provides the procedures for installing and configuring new Secure Path components into an existing RA7000/ESA10000 (SCSI) RAID storage configuration.

These procedures require that you have:

- Previously installed your RAID system into a single host/single path, or dual host/single path configuration
- Created storagesets on the RAID system using SWCC CLI
- Partitioned and formatted disk drives with the Windows NT Disk Administrator

IMPORTANT: Secure Path only supports SCSI RAID Arrays with Windows NT 4.0. Windows 2000 is NOT supported in SCSI configurations.

Secure Path (SCSI Installation) Prerequisites

Table 4-1 lists the basic requirements to support a SCSI Secure Path installation. Verify that you have received the Secure Path software kit and the SCSI hardware ordered for your installation topology. If you are missing any component, please contact your account representative or call the Compaq Customer Services Hotline at (800) 354-9000.

Table 4-1
Secure Path (SCSI Installation) Prerequisites

| Host Feature | Requirement |
|--|--|
| Platform | Intel |
| Operating System | Windows NT Enterprise Edition, Version 4.0 |
| Secure Path Software Kit | SANworks Secure Path v3.1 Enterprise Edition for Microsoft Windows (QB-669AD-SA) |
| RAID Storage System(s) | StorageWorks dual-redundant RA7000/ESA10000 (Ultra SCSI) |
| Solution Platform Kit | StorageWorks HSZ70 Solution Software for Windows NT –Intel (QB-5SBAE-SA) |
| StorageWorks Command Console | Storage management software |
| Host Bus Adapter(s) (and adapter driver) | Adaptec AHA-2944UW |
| Interconnect Hardware | As required |
| RAID Hardware | Cables supplied with the RAID system |
| Service Tools | Appropriate tools to service your equipment |
| Technical Documentation | The reference guides for your RAID system, the host server and the Windows NT software supplement this installation guide. |
| Configuration-Specific SCSI Interconnect Kit | SWXKT-EA –Ultra SCSI Hub Cluster RAID Kit SWXKT-FA –RAID SCSI Connection Kit SWXKT-DF –Cluster RAID Connection Kit |

RAID System Preparation

This section describes how to prepare your RAID system for a Secure Path environment. The specifics vary, depending on whether you are adding Secure Path capability to a new or existing SCSI RAID configuration.



WARNING: If your RAID System is in a production environment, and you intend to convert to Secure Path operation, make sure all users have logged off the server and all I/O to the RAID system has ceased before proceeding.

Preparing Existing RAID Systems for Secure Path Operation

For each RAID Array currently in use in a production environment, that you plan to reconfigure for Secure Path operation, follow normal procedures to backup the data stored on your RAID Array.

Preparing New RAID Systems for Secure Path Operation

Prepare each new RAID system in your Secure Path installation by performing the following steps.

1. Install the RAID system in a single path configuration according to the platform/solution kit documentation.
2. Using the SWCC, or the CLI utility, establish your desired storageset configuration.
3. Use Windows NT Disk Administrator to partition and format the storagesets.

Examining the Current Single Path

The next step is to ensure the existing single path configuration conforms to Secure Path requirements. Confirm that the existing storage infrastructure is robust as follows:

1. Verify that there is a serial connection to the storage system, and that you can communicate to it with SWCC or the CLI.
2. Check the Windows NT Event Log and verify no errors reported by the host adapter, or HszDisk.

3. Verify that the Windows NT system (boot) disk is not part of the storage system.
4. Verify that the server has the TCP/IP protocol installed and that the server is available on the network by pinging it.

Secure Path Installation for SCSI



WARNING: Follow normal procedures to power off your server(s) prior to installing or cabling hardware components.

Perform the following tasks in sequence to configure Secure Path hardware components:

- Preparation and installation of SCSI HBAs
- Cable the SCSI hardware components

Preparing and Installing SCSI HBAs

Secure Path installation requires that at least one additional SCSI HBA (Adaptec AHA2944UW) be installed in the host server. Before installing a SCSI HBA, prepare it for Secure Path operation as follows:

1. Set/Verify SCSI Host Adapter Termination - 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 HBA.
2. Disable SCSI Bus Reset - SCSI bus resets following board initialization (power-on reset) are **disabled**.
3. Disable SCSI Host Adapter BIOS - SCSI HBA BIOS is **disabled**.
4. Set Start Unit to “NO.”

Refer to the documentation supplied with your SCSI HBA to configure these parameters. Adapter settings must be identical for each HBA.

Follow the adapter vendor’s recommended procedure to install the additional SCSI HBAs into your server.

Cabling and Termination

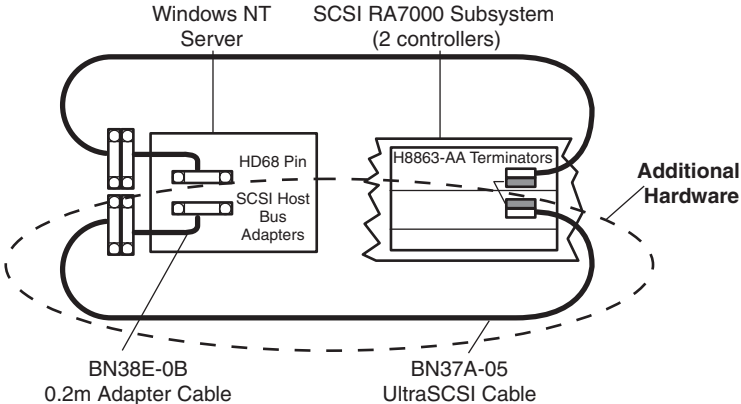
Identify your desired Secure Path hardware configuration from the descriptions listed below and locate the corresponding subsection for procedures to install Secure Path hardware configuration.

- Installing an RA7000 or ESA10000 (SCSI) and One Windows NT Server
- Installing an RA7000 or ESA10000 (SCSI) and a Windows NT Cluster with Y-Cables
- Installing an RA7000 or ESA10000 (SCSI) and a Windows NT Cluster with SCSI Hubs

Installing an RA7000 or ESA10000 (SCSI) and One Windows NT Server

To establish two individual SCSI buses between a single Windows NT 4.0 host server and a RAID system, 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 connecting both HSZ70 RAID controllers in the system.
3. Connect a terminator (H8863-AA) to the remaining tri-link connector of the controller that is currently connected to the host server.



SHR-1562

Figure 4-1. Secure Path hardware interconnect – SCSI single server

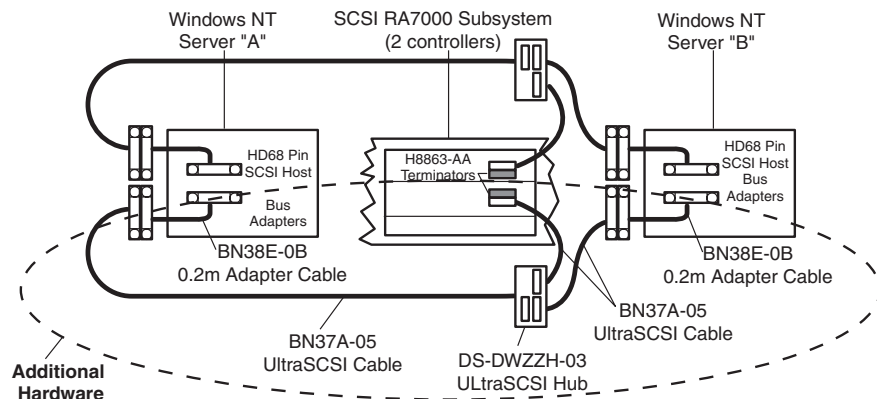
3. Move one of the existing VHDCI cables from the bottom controller to the top controller. Both connectors on the bottom controller should now be unused.
4. Attach Y-cables to each of the new HBAs, one new adapter in each server.
5. Attach SCSI terminators to one end of each Y-cable.
6. Attach the (compatible) 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)
7. Attach the VHDCI/HD68 5-meter cable between the remaining Y-cable and the bottom controller.
8. Restart the host servers.

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

Installing an RA7000 or ESA10000 (SCSI) and a Windows NT Cluster with SCSI Hubs

To establish two individual SCSI buses between clustered Windows NT 4.0 host servers and a RAID system, where one bus currently exists, reference Figure 4-3 and follow these steps:

1. Install the HBA in the servers.
2. Remove the link cable interconnecting both HSZ70 RAID controllers in the storage system.



SHR-1564

Figure 4-3. Secure Path hardware interconnect – SCSI cluster hub

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. Restart the host servers.

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

Verifying the Secure Path Hardware Configuration

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

You have now completed the configuration procedures required to support the new Secure Path environment. See Chapter 6, “Managing Secure Path,” for more information on monitoring and managing Secure Path activity using the Secure Path Manager.

Chapter 5

Installing Secure Path Software

This chapter provides installation instructions for Secure Path software. Secure Path consists of the following individually installed components:

- Server software - RaiDisk filter driver, HszDisk (Windows NT 4.0 only) class driver, and Secure Path Agent
- Client software - Secure Path Manager GUI

NOTE: The setup program automatically detects the server operating system (Windows NT 4.0 or Windows 2000), and installs accordingly.

NOTE: You must run the Fibre Channel software setup before installing Secure Path.

Server Software Installation

Install Secure Path Server software on the Windows host system to which the RAID storage system is connected. TCP/IP installation is a requirement for the host system.

IMPORTANT: The installation of Secure Path requires that a Temp directory be available on the system drive, for either Windows NT 4.0 or Windows 2000. For example: C:\Temp

Install the Secure Path Server software as follows:

1. Insert the Compaq SANworks Secure Path Software v3.1 for Microsoft Windows CD into your CD-ROM drive.
2. If you have AutoRun enabled on your server, the Secure Path setup program will start automatically. Otherwise, Choose “Run” from the START menu and enter the following command:

drive_letter:\spinstal\setup.exe

where: *drive_letter* is the drive letter assigned to the CD-ROM

The setup program automatically detects the server operating system (Windows NT 4.0 or Windows 2000), and installs accordingly.

3. When the setup starts, choose the destination path. Then choose the “Secure Path Server Install” option to install the required drivers and Agent on your server.

The Server Install option prompts you to designate clients permitted to manage the host. Setup, by default, lists the proper DNS name to use for accessing the local host from a client (Secure Path Manager) running on the local host. For cluster configurations, setup will include the local host names for each cluster member.

Check with your system administrator to assure proper TCP/IP network configurations and protocols.

4. Enter a validation password. For cluster configurations make sure the password is the same for each member of the cluster.

Client Software Installation

Install Secure Path Client software on either the same Windows host system as the Server software, or any Windows (TCP/IP-capable) workstation

Install the Secure Path Client software as follows:

1. Insert the SANworks Secure Path Software v3.1 for Microsoft Windows CD in your CD-ROM drive.
2. If you have AutoRun enabled, the Secure Path setup program will start automatically. Otherwise, Choose “Run” from the START menu and enter the following command:

drive_letter:\spinstal\setup.exe

where: *drive_letter* is the drive letter assigned to the CD-ROM

The setup program automatically detects the client operating system (Windows NT 4.0 or Windows 2000), and installs accordingly.

3. When the setup starts, choose the destination folder. Then choose the “Secure Path Client Install” option to install the Secure Path Manager software.

You have now completed the software installation procedures required to support the Secure Path environment. See Chapter 6, “Managing Secure Path,” for information on monitoring and managing Secure Path activity using Secure Path Manager.

Chapter 6

Managing Secure Path

This chapter provides the following Secure Path Manager operational information:

- Launching Secure Path Manager
- Logging on to Secure Path Manager
- Monitoring host connections
- Managing storagesets and paths
- Detecting and identifying path and controller failures
- Responding to failover events
- Reference materials for MSCS and OPS clusters

You can use Secure Path Manager (SPM) to monitor and manage a Secure Path environment. SPM displays specific information about the state of RAID storage systems and I/O paths configured for high-availability storage access. Use SPM to set various properties and modes associated with a managed storage profile, and to set failback policy. SPM automatically detects and indicates path failures, and provides the capability to move RAID Array storagesets across controller pairs to facilitate static load balancing.

Launching Secure Path Manager

To launch SPM:

1. From the START menu, select Programs, then SecurePath, and then the SPM submenu.
2. Click the Secure Path Manager (SPM) application icon.

Logging on to Secure Path Manager

Logging on to SPM incorporates entering user and storage profiles definitions directly from the login window.

Defining SPM Storage Profiles

SPM displays a *storage-centric* view of Secure Path managed RAID storage resources. All Secure Path protected RAID storage systems common to a given host (or set of hosts) are presented in an SPM display.

During SPM login, enter hosts that share these RAID storage systems while defining storage profiles from the login window.

- To create a non-clustered host profile, start by entering a host name (or set of host names) in the “Host-Cluster Names” field.
- To create a clustered-host profile, enter a host name (or set of host names) with each followed by a “-your clustername” designation to identify cluster membership.

A single instance of SPM is capable of managing:

- Multiple non-clustered hosts sharing one or more RAID storage systems
- Multiple sets of clustered-hosts sharing one or more RAID storage systems

More than one instance of SPM is required to manage installations that include a mix of non-clustered and clustered-hosts.

Figure 6-1 shows an example of an SPM login display.

Secure Path Login

Please enter Host Nodes, Cluster, Password and Profile name information:

Nodes:
Enter Hostname and Clustername (if any) separated by '-' (Hyphen)

Host-Cluster names

- sportster-MotorCars
- roadster-MotorCars
- tomcat-Fighters
- falcon-Fighters

Profile(s)
HighPerformance

Save Profile New

Password
xxxx

Save Password

Exit Help Login

Figure 6-1. SPM login window with a clustered host storage profile

After you have added all the host names to your storage profile, enter the connection password in the “Password” field. This is the password that you defined for the Secure Path Agent during setup, or when you run the Secure Path Agent Configuration utility after installation.

SPM uses this password to establish a network connection with the Secure Path host(s). For storage profiles including more than one host, the connection password must be the same on each of the Secure Path host(s).

Check “Save Password” if you want SPM to use the saved password automatically each time you login with this storage profile.

Saving an SPM Storage Profile

To save an SPM profile:

1. Enter a unique name in the “Profile(s)” field once you have defined a storage profile.

2. Save the profile by clicking “Save Profile.”

Creating A New SPM Storage Profile

To create additional SPM storage profiles:

1. Click “New.”
2. Add host name(s) in the “Host-Cluster Names” field.
3. Enter a profile name in the “Profile(s)” field.
4. Click the “Save Profile” button.

Selecting an Existing SPM Storage Profile

To choose an existing SPM storage profile, use the pull down arrow on the “Profile(s)” box to find and select the profile.

If you did not choose to save the password when you originally created the profile, enter the password in the “Password” field and click “Login.”

Editing an Existing SPM Storage Profile

To edit an existing storage profile, select the profile to be edited. Make the desired changes to the profile and click “Save Profile.”

Changing the Secure Path Agent Password

To change the Secure Path Agent’s password:

1. Run the Secure Path Agent Configuration utility located in the Secure Path program folder from the Start Menu.
2. Once you have changed the Agent’s client (SPM) access list or password using the Configuration utility you must stop and restart the Agent using the Windows Services Applet located in Control Panel.
3. Find and select the Secure Path Agent in the list of services and click “Stop.”
4. Once the Agent has stopped, select Secure Path Agent again and click “Start.”

The Agent will now restart and update its client and/or password database. Make sure that you do this for each of the hosts in an SPM storage profile.

Troubleshooting Connection Problems

If you experience problems attempting to log on to SPM, see Chapter 8, “Troubleshooting Secure Path Connection Problems,” for more information.

Monitoring Host Connections

SPM monitors connection status for each active host that is a member of the current storage profile.

As shown in Figure 6-2, a server icon is displayed for each host in the window frame located immediately below the tool bar. The host’s name is listed above the icon and a cluster name is listed below if it is a member of a cluster.

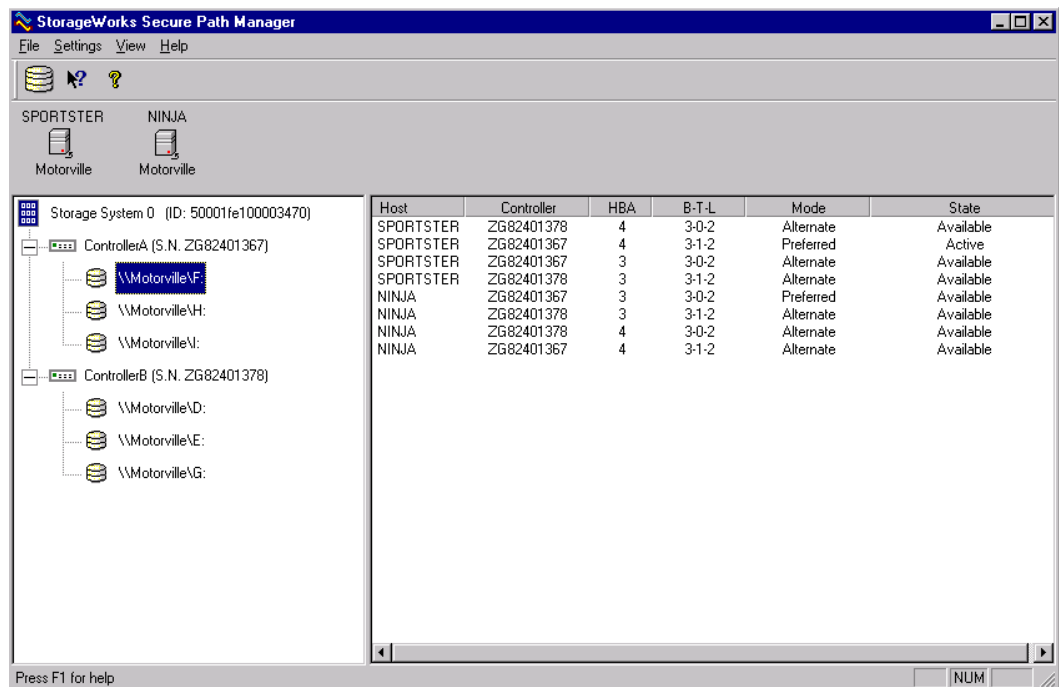


Figure 6-2. Host connection monitor

SPM monitors its connection with each member of a storage profile and will indicate a loss of connection to a particular host with a red “X.”

Figure 6-3 shows that SPM has lost connection to the Motorville cluster member Sportster.

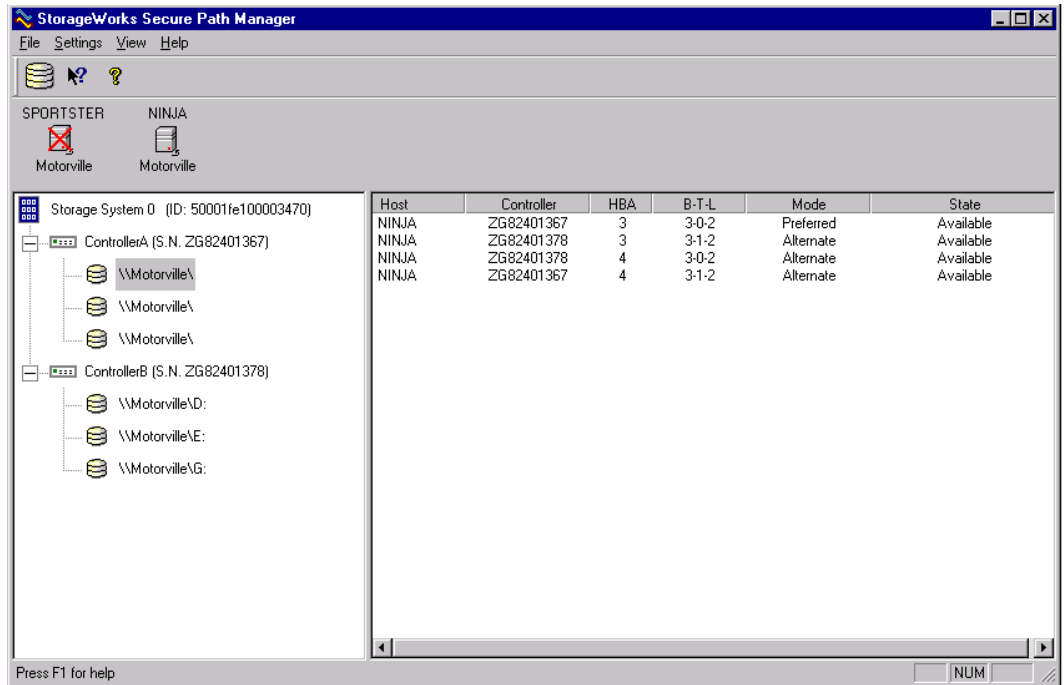


Figure 6-3. Lost host connection Icon

Responding To A Lost Host Connection

When investigating possible problems with lost host connections consider the following:

- A loss of connection does not necessarily mean that you have lost Secure Path's protection capability for storage on that host. If the host is still running, the problem is most likely due to a network connectivity problem and you have only lost Secure Path remote management functions. Secure Path's RaiDisk multiple path driver is still protecting availability to your storage.
- If the host is a member of a cluster, SPM will continue to report storage information based on data received from the surviving host or hosts.
- If the host is a member of a cluster, check your cluster management utilities to determine whether storage resources have failed-over to a surviving host.

- If the host is still running or following a reboot, run Windows Event Viewer and examine the Application and System logs to determine what happened prior to and during the loss of connection. In particular, check for network issues that may have caused a connectivity problem between the host and the SPM client.
- SPM will automatically re-establish communication to a host when the connection becomes available.

Setting Storage Profile Properties

After logging-on to SPM for the first time, examine and adjust the *Properties* settings for the current storage profile. It is important to note that these *Properties* have a global effect on all resources managed by an SPM storage profile. Using the Properties pull-down menu you can:

- Enable or Disable the **Auto-Failback** policy (default = *disabled*). When Auto-Failback is enabled, all storagesets that have failed-over to an alternate path will automatically failback to their Preferred path when access to that path is restored. Storagesets will failback automatically only if I/O operations to those storagesets are in process. Auto-failback enabled in conjunction with Path Verification enabled, permits failback to occur for quiescent storagesets.
- Enable or Disable **Load Distribution** (default = *disabled*). Load Distribution allows multiple paths between a host and a specific storageset to be used in parallel for I/O, in order to maximize performance potential. Note that Load Distribution is disabled in Microsoft Cluster Server (MSCS).
- Enable or Disable **Path Verification** (default = *enabled*). With Path Verification enabled Secure Path periodically runs diagnostics on all Preferred and Alternate paths to determine their current state. If a path is diagnosed with a problem that would prevent reliable I/O operations to complete, it is marked as FAILED and no further I/O operations are permitted on that path.
- Set the **Polling Interval** (default = *90 seconds*) to determine the rate at which SPM will request configuration change information from the Secure Path Agent(s) in the storage profile. Polling Interval only affects the rate at which displayed information is updated and has no affect on the current configuration. The Polling Interval is user selectable from a minimum 5 seconds to a maximum of 30 minutes.

Storage System View

Physical storage objects are displayed in the SPM Storage System view located in the left frame (Figure 6-4). Browsing this view will display each of the RAID storage systems, controllers, and associated storagesets that comprise your Secure Path storage profile. Objects in the Storage System view are identified as follows:

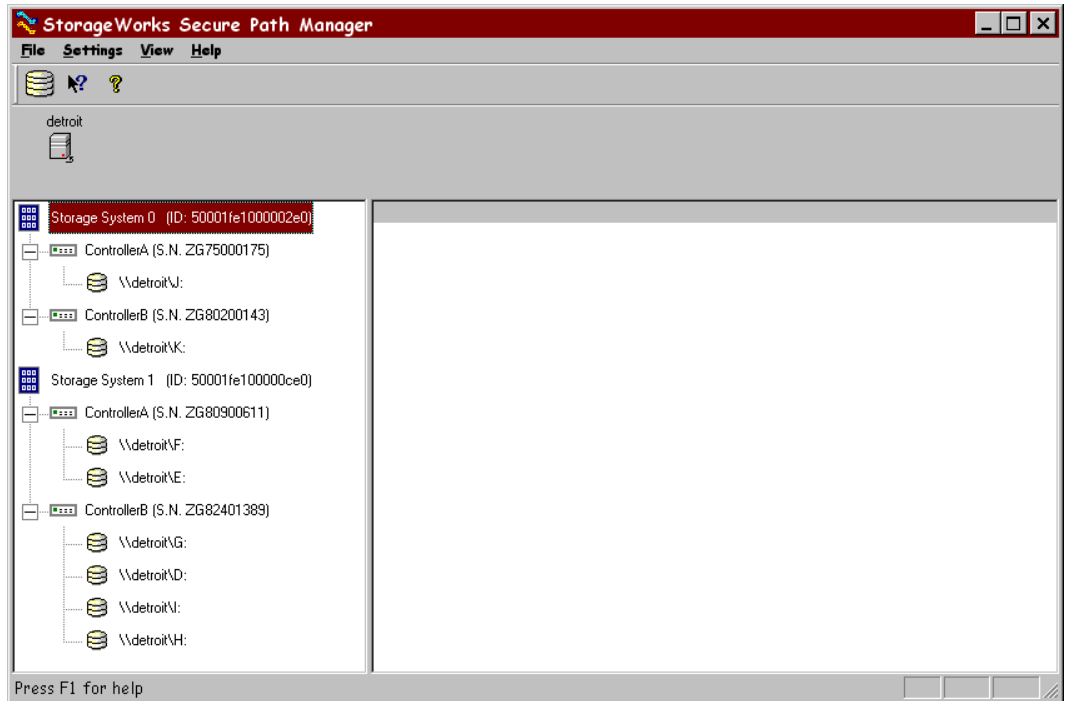


Figure 6-4. SPM single host storage profile –Storage System view

Storage Systems and Controllers

- Storage System ID** - Each RAID Array storage system is identified by a unique 64-bit value. For RA7000/ESA10000, the Storage System ID is generated by Secure Path and is derived from the controller serial numbers.

If an RA7000/ESA10000 controller is swapped, the Storage System ID will change. For an RA8000/ESA12000, the Storage System ID is determined at time of manufacture and stored in controller VRAM. The Storage System ID for RA8000/ESA12000 remains constant for the life of the RAID storage system.

- **Controller Serial Number** - The individual controllers of a RAID Array storage system are identified by a unique 10 place alphanumeric value assigned during controller manufacture.

RAID Array Stagesets

- **Disk LUN UUID** – a unique 128-bit value assigned by Secure Path.
- **Disk Number** – the logical disk number assigned by the Windows Disk Administrator.
- **Drive Letter** – the logical drive letter assigned by the Windows Disk Administrator.
- **Bus/Target/LUN** – the physical address representing the connection to the host server.
- **Volume Label** – the label assigned to the volume by the user with Windows Explorer or Disk Administrator.

You may select the method SPM uses to identify stagesets with the “View” pull-down menu located above the toolbar. SPM will always display the owning host’s name, or clustered name (for clustered hosts) along with whatever stageset identifier you choose.

Physical Path View

When you highlight a stageset from the Storage System view, SPM displays information about the physical paths that have been configured for access to that stageset in the right-hand frame. The Physical Path view includes the following information for each path:

- **Host** – is the Secure Path host system, which has an established access path to the stageset.
- **Controller** – is the RAID storage system controller servicing the path.
- **HBA** – represents the physical port number of the Host Bus Adapter servicing the path. The HBA is a relative number determined by the Windows “order of discovery” for adapters on that host.
- **B-T-L** – the physical Bus, Target, and LUN number describing the path address for the stageset.
- **Mode** - A user selectable parameter that specifies path behavior during nominal and failure conditions. Path mode may be set to Preferred, Alternate, Pre-Offline (Preferred and Offline), or Alt-Offline (Alternate and Offline).

- **State** – A set of attributes that describe the current operational condition of the path. Paths may exist in Active, Failed, or Available states.

The SPM screen (Figure 6-5) shows a single host configuration with the host “Detroit” attached to two Secure Path protected RAID storage systems. Browsing the controllers of Storage System 1 shows two storagesets owned by controller A, and four storagesets owned by controller B.

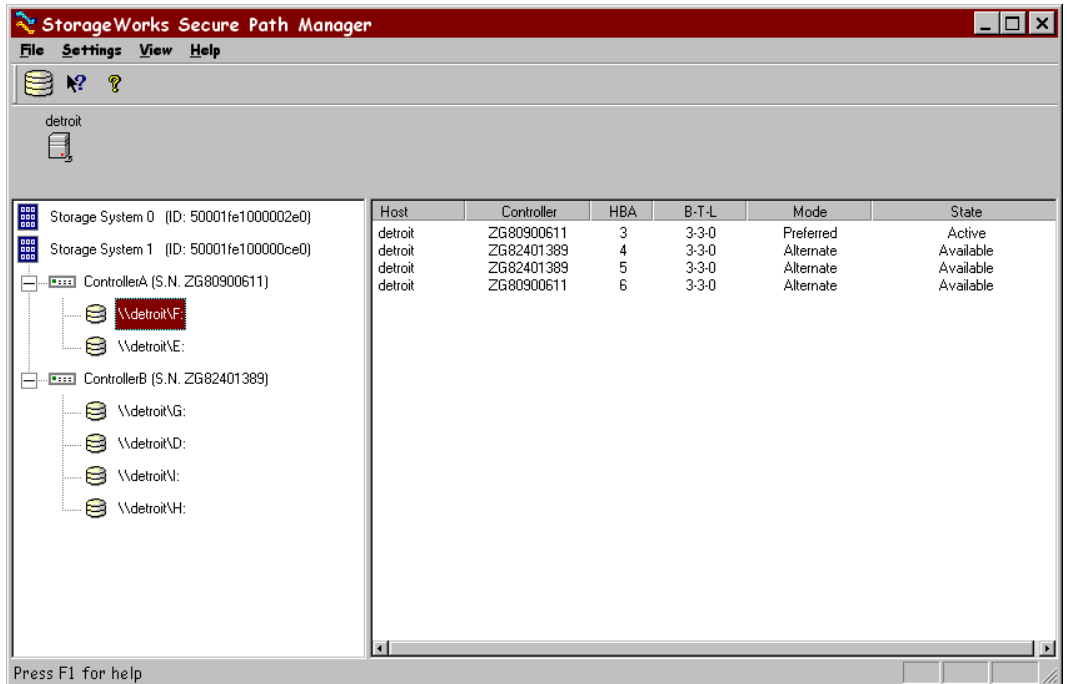


Figure 6-5. SPM single host storage profile – Physical Path view

The storageset with Windows logical drive letter F is highlighted in the Storage System view and its corresponding physical path information is presented in the right-hand frame. Each line in the Physical Path view represents a discrete path to this particular storageset.

The display information in this example shows four paths configured from host “Detroit” to drive F. One of the paths access the storageset at Bus 3, Target 3, and LUN 0 through the HBA at Port 3. One through Port 4, another through Port 5, and the last through Port 6.

Information for the first path indicates that it is in a Preferred mode and Active State. The initial starting state is derived from the controller’s preferred path attribute or the last owning controller. The Preferred mode is selected by a user

for a given path, to specify its use for all I/O operations during normal conditions. A path with a Preferred mode that is in the Active State is one that is currently used for access to a storageset under normal operating conditions.

Information from the second, third, and fourth lines of this path view indicate that these paths are in an Alternate Mode and Available State. The Alternate Mode is selected by a user for a given path, to specify its use for access to a storageset only after all Preferred paths have failed. A path with an Alternate Mode that is in the Available State is one that is currently ready to be used for access to a storageset in the event that a Preferred path fails.

The controller serial number displayed for the Preferred path is the same as the one shown in the Storage System view for the controller owning drive F.

Two of the paths in the Available State have a different serial number than that of the Preferred Mode path, indicating that they are providing standby access through the other controller. Should the controller currently servicing the Preferred path completely fail, one or more of the paths on the surviving controller will transition to the Preferred State, depending on whether or not Load Distribution has been enabled.

Polling Interval and Display Refresh

To keep the displayed path status current, SPM will periodically request updates from all Secure Path hosts. To minimize network traffic, SPM performs display updates only when a configuration change is reported and updates only the information that has changed. The rate at which status changes are requested is determined by the Polling Interval that you set from the Properties menu.

A display Refresh operation, which you invoke through use of the View menu item or with the F5 hotkey, causes SPM to request fresh configuration information from all hosts included in the storage profile. SPM updates all displayed information in response to a Refresh request. Since a Refresh will update the entire display, it can take longer to perform than a normal polling operation. How long the Refresh takes will depend upon the number of hosts, RAID storage systems, and storagesets in the monitored storage profile.

Managing Storagesets and Paths

You can perform the following actions on the storagesets and paths managed by SPM:

- Move a storageset from one controller to the other
- Make a path Alternate
- Make a path Preferred
- Change the Preferred path
- Make a path Offline
- Make a path Online
- Verify a path
- Repair a path

Moving A Storageset

Choose *Move a Storageset* when you want to change the ownership from the current RAID Array controller to the other. This action is useful if you need to balance I/O loading across controllers or to manually return a failed-over storageset to its Preferred path when Auto-Failback has been disabled.

There are two methods available to move a storageset.

1. Click the drive to highlight it in the storage system view.
2. Drag the drive to the other controller or right click to select the “Move To Other Controller” action.

Making A Path Alternate

Choose *Make a Path Alternate* when you have Load Distribution enabled and you want to disable I/O operations to one or more paths. To make a path Alternate:

1. Click the Preferred path you wish to change.
2. Right click to select the “Make Alternate” action.

Making A Preferred Path

Choose *Make a Path Preferred* when you have Load Distribution enabled and you want to re-enable I/O operations to a path that you have previously disabled using “Make Alternate.” To make a path Preferred:

1. Click the Alternate path you wish to change.
2. Right click to select the “Make Preferred” action.

Changing A Preferred Path

Choose *Change a Preferred Path* when Load Distribution is disabled. There are multiple paths available to a storageset on the same controller and you wish to select a new Preferred path for normal I/O operations. To change a Preferred path:

1. Click the Alternate path you wish to change to Preferred.
2. Right click to select the “Change Preferred” action.

Making A Path Offline

Choose *Make a Path Offline* when you want to prevent that path from being used for any I/O operations under any circumstances. For instance, use the Offline mode when you need to replace or work on a storage interconnect component. To make a path Offline:

1. Click a Preferred or Alternate path.
2. Right click to select the “Make Offline” action.

If the path was an Alternate, its mode will change to Alt-Offline. If the path was Preferred, its mode will change to Pre-Offline.

Making A Path Online

Choose *Make a Path Online* when you want to return a path that is currently in the “Alt-Offline” or “Pre-Offline” mode to its original mode. To make a path online:

1. Click a path in the “Alt-Offline” or “Alt-Online” mode.
2. Right click to select the “Make Online” action.

If the path was Alt-Online, its mode will change to Alternate. If the path was Pre-Offline, its path will change to Preferred.

Verifying A Path

Choose *Verify a Path* when you want SPM to determine the current state of a path. To verify a path:

1. Click the path.
2. Right click to select the “Verify Path” action.

SPM will generate a pop-up message when the verification completes to indicate the result of the operation. No state change will occur as a result of this operation.

Repairing A Path

Choose *Repair a Path* when you want SPM to restore access to a failed path after the problem has been corrected. To Repair a path:

1. Click a path in the FAILED State.
2. Right click to select the “Repair Path” action.

If the Repair action is completed successfully the path’s state will change to Available if its mode is Alternate, or Active if its mode is Preferred.

Detecting and Identifying Path and Controller Failures

SPM periodically monitors the status of all systems in your storage profile at a rate determined by the Polling Interval. To indicate failures, icons are used in the Storage System view and path states are set to FAILED in the Physical Path view.

In addition, failover events are logged by the RaiDisk driver in the Windows Event Viewer. The Secure Path Agent will also notify SWCC clients immediately when a fault is detected.

You should routinely monitor SPM status to check for occurrences of failover events that might compromise either the performance or availability of storage resources. For example, if you use Load Distribution to enhance the performance of your storage resources, this capability may be diminished if

one or more of your Active paths are lost due to component failure. Also, availability is compromised if your configuration includes only two configured paths to a storageset and one is lost due to component failure. Secure Path will be unable to failover to a redundant path should a subsequent fault occur in this situation.

The SPM client is not required to be running in order for Secure Path to protect path availability. The RaiDisk device driver running on the host handles Secure Path's automated path protection capability.

Detecting Path Failures

Several types of icons appear in the SPM display to indicate the presence of a path failure. Recognizing these icons will help you to determine the specific storageset and path associated with the failure. The icons shown below are displayed in the storage System View to indicate that a path failure has been detected by Secure Path.

Storage System Path Failure Detected

The icon shown in Figure 6-6 indicates that a failure of at least one, but not all paths to that RAID Array storage system was detected by Secure Path. Browse the storage system to determine the affected controller and storagesets.



Figure 6-6. Storage system path failure detected

Storage Controller Path Failure Detected

The icon shown in Figure 6-7 indicates that a failure of at least one, but not all paths to that storage controller was detected by Secure Path. Browse the storage controller to determine the affected storageset(s).



Figure 6-7. Controller path failure detected

Unless you have the Path Verification property enabled, Secure Path only detects failures for paths with active I/O. This means that it is possible that one or more paths may be failed to other storagesets owned by the same controller, but not yet detected by Secure Path. However, Secure Path will perform path or controller failover of these drives, and indicate the failure if subsequent I/O occurs to any or all of the storageset(s).

If you have Path Verification enabled, Secure Path will automatically detect the failure of paths to all of the affected storagesets on the controller and immediately perform whatever path or controller failover activity is necessary to maintain availability.

Storageset Path Failure Detected

The icon shown in Figure 6-8 indicates that a failure of at least one, but not all paths to that storageset was detected by Secure Path. Click on the storageset to highlight it and examine the Physical Path view information to determine the specific nature of the path failure.



Figure 6-8. Storageset path failure detected

Total Path Failures

Each of the icons shown below indicates that all paths to the affected storage object have failed.



Figure 6-9. Storage system failure detected



Figure 6-10. Storage controller failure detected



Figure 6-11. Storageset failure detected

Identifying Path Failovers

To identify the source of path failover activity, first check the Storage System view for path failed icons, then examine the Physical Path view of the affected storageset. Check for paths that indicate FAILED status. Whether you see one or more paths to a particular storageset in the FAILED state, will depend upon the following conditions:

- Was I/O active on the affected storageset?

Secure Path determines path failures by detecting the failure of I/O operations to complete. This means that if I/O was not active on a broken Preferred path, the fault will not be detected and the path's state will not be marked as FAILED until I/O operations occur.

- Is Path Verification enabled?

Path Verification periodically tests the viability of all paths and will automatically detect faults on all Preferred and Alternate paths. This means that a controller failover on installations with multiple paths to a storageset, will result in FAILED states for both the Preferred and Alternate paths to the failed controller.

- Is Load Distribution enabled with more than one Preferred path?

When you enable the Load Distribution property, Secure Path makes each Available path to a storageset through the owning controller a Preferred path.

When Load Distribution is enabled and a single path failure occurs, Secure Path will change only the failed Preferred path to the FAILED state. When Load Distribution is enabled and a controller failover occurs, Secure Path will change each of the Preferred paths to FAILED state.

Identifying Controller Failovers

A RAID Array controller failure will cause Secure Path to change the ownership of a given storageset to the surviving controller. Failover will occur only for those storagesets with active I/O operations. If you suspect that a controller failover has occurred use the Path Verification feature to check the viability of all configured paths. Although you may enable it at anytime, Path Verification will require approximately two minutes per storageset to verify the integrity of all paths in the storage profile.

The Path Verification diagnostics will identify the specific failing controller in the Storage System view. Check for the failed storage controller icon shown in Figure 6-10. SPM will show that all storagesets previously on this controller have been failed-over to the surviving controller. Because all of the Alternate paths to the faulty controller have transitioned to the FAILED State because of Path Verification, storageset path failure icons will be displayed for each storageset on the surviving controller.

Responding to Failover Events

When investigating possible problems with failovers, consider the following:

- Are there additional Available paths remaining to the storageset or has this failure totally eliminated the ability to survive any subsequent failures?

- If you have Load Distribution enabled, are other paths or controllers suffering degraded performance due to the increased load placed on the remaining paths?
- What caused the failure?

Most storage channel problems are caused by failures in the interconnect hardware. To determine what occurred prior to, and during a failure, examine the Windows Event Viewer and review the System log for events entered by the RaiDisk and/or host bus adapter device drivers. Check the Application Log for events entered by the Secure Path Agent and SPM. Use StorageWorks Command Console to check for RAID array system faults. Visually inspect your switches or hubs for LED or LCD hardware fault indications.

Using SPM with MSCS and OPS Clusters

The two clustering models employed by Microsoft Cluster Server (MSCS) and Oracle Parallel Server (OPS) result in different SPM Preferred path status indications for shared storagesets. The differences in these cluster implementations is associated with the way in which the two systems manage their shared resources and also prohibits the use of Load Distribution in MSCS environments.

However, the SPM display for both cluster types will always show the associated cluster name alongside the storageset in the Storage System view. When you highlight a storageset, SPM will display all of the physical paths from each cluster host to that particular storageset in the Physical Path view.

Microsoft Cluster Server Environments

Microsoft Cluster Server uses hardware device reservation as a mechanism to synchronize drive access. Device reservation means that a shared storageset is in effect “owned” by a single cluster host at any given time. You can determine the owning host from SPM by looking for the storageset path in the Active State. A non-owning host is indicated by a storageset path in the Preferred mode and Available State. Since Load Distribution is automatically disabled in MSCS environments, this is the only configuration possible for Preferred paths under nominal operating conditions.

Oracle Parallel Server Environments

Oracle Parallel Server allows multiple instances on different hosts to mount and access the same database files. Oracle Parallel Server uses a Distributed Lock Management mechanism to synchronize and control attempts by two or

more hosts to modify the same information simultaneously. In an OPS cluster environment all hosts effectively “own” all shared storagesets all the time. This means that when you view a storageset from the Physical Path view each member of the OPS cluster will have a path to that drive in the Preferred mode and Active state.

Chapter 7

Using Secure Path with SWCC

This chapter provides the following Secure Path and StorageWorks Command Console (SWCC) interoperability information:

- Adding Secure Path to the network
- Using SWCC to monitor the Secure Path system

SWCC is a Windows-style GUI that uses standard Windows navigation features and command selection. Folders are used to arrange Secure Path managed storage systems and non-Secure Path managed storage systems.

The SWCC Navigation Window provides a list of all the host computers and storage systems to which SWCC is connected. You can use the Navigation Window to monitor storage systems for failures. SWCC will monitor your network connection and storage system and report status by changing the icons in the Navigation Window.

Adding a Secure Path System to the Network

To add a Secure Path System to the network:

1. From the SWCC File menu, click *Add System*.
2. Enter a Domain Name Service (DNS) name or the IP address in the *Host name or TCP/IP address*: text box.
3. Click *Apply*. After you click *Apply*, the SWCC Client adds an icon in the Navigation Window for the host running the Secure Path Agent.
4. Click *Close* when the second *Add System* dialog box appears.

When SWCC connects to a Secure Path system, it will add the following folders in the Navigation Window:

- Host Folder – which has the host name
- Storage System Folder
- SPM Window

The SPM window does not support the launching of Secure Path Manager (SPM). To launch SPM, select the SPM icon from START/Programs/Secure Path submenu.





NOTE: Attempting to launch SPM from the SWCC Navigation Window will result in an error generated by the Applet Manager, stating an object creation failure.

Using SWCC to Monitor the Secure Path System

SWCC monitors all storage systems displayed on the Navigation Window. Failures occurring in the Secure Path system are indicated in the Navigation Window by a change in the appearance of the controller folder icon, as defined in Table 7-1.

A Controller Folder shows all the storage associated with a controller. Table 7-1 lists the four states of a Controller Folder.

Table 7-1
Controller Folder States

| Controller Folder Icon | State |
|---|---|
|  | The Secure Path system contained in this folder is working properly. |
|  | A Secure Path component has failed. For details, launch SPM from the START/Programs/Secure Path menu. |
|  | A grayed out folder indicates no connection to the Secure Path Agent. |
|  | <i>This state is not currently supported by Secure Path software.</i> |

NOTE: A failure indicated by a change in the controller folder icon will also be reflected in the corresponding host folder icon.

SWCC offers a variety of methods for notifying the user about any system failures. For details of error notification and other SWCC related issues, consult your Solution Software kit's *Compaq StorageWorks Command Console Guide* that supports the RAID storage system.

Chapter **8**

Troubleshooting Secure Path Connection Problems

This chapter provides the following Secure Path network connectivity troubleshooting information:

- Client/Agent considerations
- Network considerations

If further assistance is required, please contact the account representative or call the Compaq Customer Services Hotline at (800) 354-9000.

Client/Agent Considerations

The following Client/Agent considerations may be useful in troubleshooting network connection problems:

- Add each client's NetBIOS name or Fully Qualified Domain Name (FQDN) to the Agent's list of authorized clients using the Agent Configuration utility, and set the password in the Password Dialog Box. Once you have made the modifications, Stop, and Restart the Secure Path Agent to update the database using the Services applet from Control Panel.
- Make sure that you use the same name type, either NetBIOS or FQDN, during Secure Path client login that you have entered in the Agent's database.
- Each name you use must be mapped to its network IP address using one of the following:
 - *HOSTS* file (static text file with either NetBIOS or FQDN mapped to IP)
 - Windows Internet Naming Service (WINS with a NetBIOS name)
 - Domain Name System (DNS with a Fully Qualified Domain Name)

See *Network Considerations* below for more information.

- In cluster configurations make sure that the password you choose is common for both agents in the cluster.
- Secure Path does not use Windows domain authentication to authorize clients. Client authentication is handled for each Agent using name-to-IP address resolution and password verification from the Secure Path configuration database.

Network Considerations

The following network considerations may be useful in troubleshooting network connection problems:

- Client names up to 15 letters without a dot (".") can be resolved by NetBIOS broadcast resolution, as long as the client and agent nodes are configured on the same subnet. If the client and agent are located on different subnets then you must use the *LMHOSTS* file, *HOSTS* file, WINS, or DNS to resolve the address.

- If you use the *LMHOSTs* file, make sure that the "Enable LMHOSTs Lookup" box is checked in the TCP/IP protocol properties of the client system.

On the client system, you must enter the NETBIOS name and the IP address of the Agent you wish to connect with in the *LMHOSTs* file and save it.

Click the "Import LMHOSTs" button to specify the location of the *LMHOSTs* file. The *LMHOSTs* and *HOSTs* files are normally located in the `\system32\drivers\etc` subdirectory.

Finally, from a command prompt issue the "NBTSTAT -R" command to purge and reload the remote name table.

- Client names that exceed 15 letters or carry a dot require an entry for that name in the *HOSTs* file or resolution by a DNS server. It is also possible to have DNS resolve NetBIOS names as long as the DNS server is updated with the appropriate information. Make sure you have checked the "Enable DNS for Windows Resolution" box in the TCP/IP protocol properties of the client system.
- If you are using DNS for host name-to-IP resolution, then the DNS database on the DNS server must be updated with the appropriate information.
- For best network connection results, it is recommended that you use Fully Qualified Domain Names with DNS.
- For production environments, where management and security are a concern, it is recommended that fully qualified names be used with DNS name resolution.
- For test and evaluation environments it is usually easier to simply add the server's name to the client's *HOSTs* file and the client's name to the server's *HOSTs* file.
- Make sure that you can ping the Secure Path host, both locally and from a remote host using the host name, not the IP address.

Appendix **A**

Glossary

- Bus** For parallel SCSI configurations, the bus is a number assigned to the physical interconnect(s) emitted by an HBA.
For Fibre Channel configurations, HBAs may use multiple bus numbers as an artificial method of expanding bus address space.
- Controller** A controller is a hardware device that facilitates communication between a host and one or more LUNs organized as an array. The HSZ70 and HSG80 are array controllers supported for use with Secure Path. Each controller in an HSZ70 or HSG80 RAID system is identified by a unique serial number, which is displayed next to the controller icons by Secure Path Manager. Secure Path Manager identifies a pair of controllers configured in multiple-bus mode by a unique 64-bit identifier that is displayed next to the subsystem icon.
- HBA** An HBA (Host Bus Adapter) is an I/O device which serves as the interface connecting a host system to the SCSI bus or SAN (Storage Area Network). HBAs are assigned a relative port number by the Windows operating system according to order of discovery (see Port).
- Host** A host is a computer system on which the Secure Path server software (RaiDisk driver and Agent service) is running.
- LUN** A LUN (Logical Unit Number) is the actual unit number assigned to a device at the RAID system controller.

- Mode** Mode is a user-selectable parameter that specifies path behavior during nominal and failure conditions. Paths may be set to one of the following modes:
- **Preferred** - indicates the desired I/O path(s). When Load Distribution is enabled I/O is distributed to a LUN using all available preferred paths according to a round-robin policy. When Path Verification is enabled all preferred paths would be verified.
 - **Alternate** - indicates a path is used only for device access once all Primary Paths to the device have failed. Paths in this mode participate in path-verification, if enabled.
 - **Offline** - indicates a path that will not be used for I/O to a LUN. The Offline mode is logically or'd with one of the other two path modes.
- Path** A path is a virtual communication route that enables data and commands to pass between a host server and a storage device.
- Port** A port is the relative number of an HBA. A specific port number is determined according to its order of discovery by the Windows operating system and includes SCSI, Fibre Channel, and IDE adapter types.
- Reduced Mode** Reduced Mode is the condition of a system where one or more *redundant* components fail, but the system is operational.
- State** State is an attribute that describes the current operational condition of a path. A path may exist in the following state(s):
- **Active** - indicates a path that is currently servicing I/O requests.
 - **Failed** - indicates a path that is disabled and not actively servicing I/O requests.
 - **Available** - indicates a path that is neither Active nor Failed.
 - **Remote** - indicates a path that connects to a remote member of a PPRC (Point-to-Point Remote Copy) configuration. Remote state may be logically or'd with any of the other states.

Target For parallel SCSI configurations, the target is the actual target number assigned to a device.

For Fibre Channel configurations, the target number is assigned by a mapping function at the mini-port driver level and is derived from ALPA (Arbitrated Loop Physical Addresses) in a FC-AL topology. For a fabric topology, it is a mapping function derived from the order of discovery according to port connections at the SAN (Storage Area Network) switch.

Removing Secure Path Software

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

Removing Secure Path Software

To remove Secure Path software from your system:

1. Establish a serial connection to the storage system.
2. At the RAID storage system prompt, enter the following command:
HSZ70> set nomultibus
3. The other controller shuts down. Momentarily depress the restart button on the controller's front panel to restart the controller. Wait for the controller to restart, then enter:

HSZ70> set failover copy = this

The controllers will configure for dual-redundant operation.

4. Launch Control Panel and choose "Add/Remove Programs."
5. Select "Remove RaiDisk."
6. Click OK in the resulting window.
7. Select "Remove Secure Path Client."
8. Click OK in the resulting window.
9. Select "Remove Secure Path Server."

10. Click OK in the resulting window.
11. For FC RAID Array 8000 or ESA 12000 storage systems installed on Windows NT hosts, uninstall HszDisk by selecting "Remove HszDisk" and re-install HSZinstall from your RA8000 Windows Platform Kit.
12. For FC RAID Array 8000 or ESA 12000 storage systems installed on Windows 2000 hosts, re-install HSZinstall from your RA8000 Windows Platform Kit.
13. Shut down the system.
14. Remove redundant paths from the controller.

The Secure Path software removal process is complete.

Appendix **C**

Valid ALPA Settings

Table C-1 lists the valid ALPA settings for hard addressing the Fibre Channel Arbitrated Loop. For controller ports, select from ALPA addresses 0x71 and above. The grayed addresses are reserved.

Table C-1
Valid Arbitrated Loop Physical Address (ALPA) Settings

| | | | | | | | | |
|------|------|------|------|------|------|------|------|------|
| 0x01 | 0x02 | 0x04 | 0x08 | 0x0F | 0x10 | 0x17 | 0x18 | 0x1B |
| 0x1D | 0x1E | 0x1F | 0x23 | 0x25 | 0x26 | 0x27 | 0x29 | 0x2A |
| 0x2B | 0x2C | 0x2D | 0x2E | 0x31 | 0x32 | 0x33 | 0x34 | 0x35 |
| 0x36 | 0x39 | 0x3A | 0x3C | 0x43 | 0x45 | 0x46 | 0x47 | 0x49 |
| 0x4A | 0x4B | 0x4C | 0x4D | 0x4E | 0x51 | 0x52 | 0x53 | 0x54 |
| 0x55 | 0x56 | 0x59 | 0x5A | 0x5C | 0x63 | 0x65 | 0x66 | 0x67 |
| 0x69 | 0x6A | 0x6B | 0x6C | 0x6D | 0x6E | 0x71 | 0x72 | 0x73 |
| 0x74 | 0x75 | 0x76 | 0x79 | 0x7A | 0x7C | 0x80 | 0x81 | 0x82 |
| 0x84 | 0x88 | 0x8F | 0x90 | 0x97 | 0x98 | 0x9B | 0x9D | 0x9E |

continued

Table C-1

Valid Arbitrated Loop Physical Address (ALPA) Settings *continued*

| | | | | | | | | |
|------|------|------|------|------|------|------|------|------|
| 0x9F | 0xA3 | 0xA5 | 0xA6 | 0xA7 | 0xA9 | 0xAA | 0xAB | 0xAC |
| 0xAD | 0xAE | 0xB1 | 0xB2 | 0xB3 | 0xB4 | 0xB5 | 0xB6 | 0xB9 |
| 0xBA | 0xBC | 0xC3 | 0xC5 | 0xC6 | 0xC7 | 0xC9 | 0xCA | 0xCB |
| 0xCC | 0xCD | 0xCE | 0xD1 | 0xD2 | 0xD3 | 0xD4 | 0xD5 | 0xD6 |
| 0xD9 | 0xDA | 0xDC | 0xE0 | 0xE1 | 0xE2 | 0xE4 | 0xE8 | 0xEF |

Table C-2 lists ALPA to SCSI mapping for the StorageWorks KGPSA HBA, as implemented at the mini-port driver. There are two potential mappings based on registry parameters (ScanDown=0 or ScanDown=1). Secure Path installation requires ScanDown=1 mapping (indicated by double asterisks). For more information, refer to your KGPSA HBA documentation.

Table C-2
ALPA to SCSI Mapping

| Bus # | Target # | LUN # | *AL_PA | *SEL_ID | **AL_PA | **SEL_ID |
|-------|----------|-------|--------|---------|---------|----------|
| 0 | 0-31 | 0-7 | None | None | None | None |
| 1 | 0 | 0-7 | 0x01 | 0x7D | 0xEF | 0x00 |
| | 1 | 0-7 | 0x02 | 0x7C | 0xE8 | 0x01 |
| | 2 | 0-7 | 0x04 | 0x7B | 0xE4 | 0x02 |
| | 3 | 0-7 | 0x08 | 0x7A | 0xE2 | 0x03 |
| | 4 | 0-7 | 0x0F | 0x79 | 0xE1 | 0x04 |
| | 5 | 0-7 | 0x10 | 0x78 | 0xE0 | 0x05 |
| | 6 | 0-7 | 0x17 | 0x77 | 0xDC | 0x06 |
| | 7 | 0-7 | 0x18 | 0x76 | 0xDA | 0x07 |
| | 8 | 0-7 | 0x1B | 0x75 | 0xD9 | 0x08 |
| | 9 | 0-7 | 0x1D | 0x74 | 0xD6 | 0x09 |
| | 10 | 0-7 | 0x1E | 0x73 | 0xD5 | 0x0A |
| | 11 | 0-7 | 0x1F | 0x72 | 0xD4 | 0x0B |
| | 12 | 0-7 | 0x23 | 0x71 | 0xD3 | 0x0C |
| | 13 | 0-7 | 0x25 | 0x70 | 0xD2 | 0x0D |
| | 14 | 0-7 | 0x26 | 0x6F | 0xD1 | 0x0E |
| | 15 | 0-7 | 0x27 | 0x6E | 0xCE | 0x0F |
| | 16 | 0-7 | 0x29 | 0x6D | 0xCD | 0x10 |
| | 17 | 0-7 | 0x2A | 0x6C | 0xCC | 0x11 |
| | 18 | 0-7 | 0x2B | 0x6B | 0xCB | 0x12 |
| 19 | 0-7 | 0x2C | 0x6A | 0xCA | 0x13 | |

continued

Table C-2
ALPA to SCSI Mapping *continued*

| Bus # | Target # | LUN # | *AL_PA | *SEL_ID | **AL_PA | **SEL_ID |
|-------------|----------|-------|--------|---------|---------|----------|
| 1 | 20 | 0-7 | 0x2D | 0x69 | 0xC9 | 0x14 |
| (continued) | 21 | 0-7 | 0x2E | 0x68 | 0xC7 | 0x15 |
| | 22 | 0-7 | 0x31 | 0x67 | 0xC6 | 0x16 |
| | 23 | 0-7 | 0x32 | 0x66 | 0xC5 | 0x17 |
| | 24 | 0-7 | 0x33 | 0x65 | 0xC3 | 0x18 |
| | 25 | 0-7 | 0x34 | 0x64 | 0xBC | 0x19 |
| | 26 | 0-7 | 0x35 | 0x63 | 0xBA | 0x1A |
| | 27 | 0-7 | 0x36 | 0x62 | 0xB9 | 0x1B |
| | 28 | 0-7 | 0x39 | 0x61 | 0xB6 | 0x1C |
| | 29 | 0-7 | 0x3A | 0x60 | 0xB5 | 0x1D |
| | 30 | 0-7 | 0x3C | 0x5F | 0xB4 | 0x1E |
| | 31 | 0-7 | None | None | None | None |
| 2 | 0 | 0-7 | 0x43 | 0x5E | 0xB3 | 0x1F |
| | 1 | 0-7 | 0x45 | 0x5D | 0xB2 | 0x20 |
| | 2 | 0-7 | 0x46 | 0x5C | 0xB1 | 0x21 |
| | 3 | 0-7 | 0x47 | 0x5B | 0xAE | 0x22 |
| | 4 | 0-7 | 0x49 | 0x5A | 0xAD | 0x23 |
| | 5 | 0-7 | 0x4A | 0x59 | 0xAC | 0x24 |
| | 6 | 0-7 | 0x4B | 0x58 | 0xAB | 0x25 |
| | 7 | 0-7 | 0x4C | 0x57 | 0xAA | 0x26 |
| | 8 | 0-7 | 0x4D | 0x56 | 0xA9 | 0x27 |
| | 9 | 0-7 | 0x4E | 0x55 | 0xA7 | 0x28 |
| | 10 | 0-7 | 0x51 | 0x54 | 0xA6 | 0x29 |
| | 11 | 0-7 | 0x52 | 0x53 | 0xA5 | 0x2A |
| | 12 | 0-7 | 0x53 | 0x52 | 0xA3 | 0x2B |
| | 13 | 0-7 | 0x54 | 0x51 | 0x9F | 0x2C |

continued

Table C-2
ALPA to SCSI Mapping *continued*

| Bus # | Target # | LUN # | *AL_PA | *SEL_ID | **AL_PA | **SEL_ID |
|------------------|----------|-------|--------|---------|---------|----------|
| 2 (continued) | 14 | 0-7 | 0x55 | 0x50 | 0x9E | 0x2D |
| | 15 | 0-7 | 0x56 | 0x4F | 0x9D | 0x2E |
| | 16 | 0-7 | 0x59 | 0x4E | 0x9B | 0x2F |
| | 17 | 0-7 | 0x5A | 0x4D | 0x98 | 0x30 |
| | 18 | 0-7 | 0x5C | 0x4C | 0x97 | 0x31 |
| | 19 | 0-7 | 0x63 | 0x4B | 0x90 | 0x32 |
| | 20 | 0-7 | 0x65 | 0x4A | 0x8F | 0x33 |
| | 21 | 0-7 | 0x66 | 0x49 | 0x88 | 0x34 |
| | 22 | 0-7 | 0x67 | 0x48 | 0x84 | 0x35 |
| | 23 | 0-7 | 0x69 | 0x47 | 0x82 | 0x36 |
| | 24 | 0-7 | 0x6A | 0x46 | 0x81 | 0x37 |
| | 25 | 0-7 | 0x6B | 0x45 | 0x80 | 0x38 |
| | 26 | 0-7 | 0x6C | 0x44 | 0x7C | 0x39 |
| | 27 | 0-7 | 0x6D | 0x43 | 0x7A | 0x3A |
| 28 | 0-7 | 0x6E | 0x42 | 0x79 | 0x3B | |
| 29 | 0-7 | 0x71 | 0x41 | 0x76 | 0x3C | |
| 30 | 0-7 | 0x72 | 0x40 | 0x75 | 0x3D | |
| 31 | 0-7 | None | None | None | None | |
| 3 | 0 | 0-7 | 0x73 | 0x3F | 0x74 | 0x3E |
| | 1 | 0-7 | 0x74 | 0x3E | 0x73 | 0x3F |
| | 2 | 0-7 | 0x75 | 0x3D | 0x72 | 0x40 |
| | 3 | 0-7 | 0x76 | 0x3C | 0x71 | 0x41 |
| | 4 | 0-7 | 0x79 | 0x3B | 0x6E | 0x42 |
| | 5 | 0-7 | 0x7A | 0x3A | 0x6D | 0x43 |
| | 6 | 0-7 | 0x7C | 0x39 | 0x6C | 0x44 |
| | 7 | 0-7 | 0x80 | 0x38 | 0x6B | 0x45 |

continued

Table C-2
ALPA to SCSI Mapping *continued*

| Bus # | Target # | LUN # | *AL_PA | *SEL_ID | **AL_PA | **SEL_ID |
|-------------|----------|-------|--------|---------|---------|----------|
| 3 | 8 | 0-7 | 0x81 | 0x37 | 0x6A | 0x46 |
| (continued) | 9 | 0-7 | 0x82 | 0x36 | 0x69 | 0x47 |
| | 10 | 0-7 | 0x84 | 0x35 | 0x67 | 0x48 |
| | 11 | 0-7 | 0x88 | 0x34 | 0x66 | 0x49 |
| | 12 | 0-7 | 0x8F | 0x33 | 0x65 | 0x4A |
| | 13 | 0-7 | 0x90 | 0x32 | 0x63 | 0x4B |
| | 14 | 0-7 | 0x97 | 0x31 | 0x5C | 0x4C |
| | 15 | 0-7 | 0x98 | 0x30 | 0x5A | 0x4D |
| | 16 | 0-7 | 0x9B | 0x2F | 0x59 | 0x4E |
| | 17 | 0-7 | 0x9D | 0x2E | 0x56 | 0x4F |
| | 18 | 0-7 | 0x9E | 0x2D | 0x55 | 0x50 |
| | 19 | 0-7 | 0x9F | 0x2C | 0x54 | 0x51 |
| | 20 | 0-7 | 0xA3 | 0x2B | 0x53 | 0x52 |
| | 21 | 0-7 | 0xA5 | 0x2A | 0x52 | 0x53 |
| | 22 | 0-7 | 0xA6 | 0x29 | 0x51 | 0x54 |
| | 23 | 0-7 | 0xA7 | 0x28 | 0x4E | 0x55 |
| | 24 | 0-7 | 0xA9 | 0x27 | 0x4D | 0x56 |
| | 25 | 0-7 | 0xAA | 0x26 | 0x4C | 0x57 |
| | 26 | 0-7 | 0xAB | 0x25 | 0x4B | 0x58 |
| | 27 | 0-7 | 0xAC | 0x24 | 0x4A | 0x59 |
| | 28 | 0-7 | 0xAD | 0x23 | 0x49 | 0x5A |
| | 29 | 0-7 | 0xAE | 0x22 | 0x47 | 0x5B |
| | 30 | 0-7 | 0xB1 | 0x21 | 0x46 | 0x5C |
| | 31 | 0-7 | None | None | None | None |
| 4 | 0 | 0-7 | 0xB2 | 0x20 | 0x45 | 0x5D |
| | 1 | 0-7 | 0xB3 | 0x1F | 0x43 | 0x5E |

continued

Table C-2
ALPA to SCSI Mapping *continued*

| Bus # | Target # | LUN # | *AL_PA | *SEL_ID | **AL_PA | **SEL_ID |
|-------------|----------|-------|--------|---------|---------|----------|
| 4 | 2 | 0-7 | 0xB4 | 0x1E | 0x3C | 0x5F |
| (continued) | 3 | 0-7 | 0xB5 | 0x1D | 0x3A | 0x60 |
| | 4 | 0-7 | 0xB6 | 0x1C | 0x39 | 0x61 |
| | 5 | 0-7 | 0xB9 | 0x1B | 0x36 | 0x62 |
| | 6 | 0-7 | 0xBA | 0x1A | 0x35 | 0x63 |
| | 7 | 0-7 | 0xBC | 0x19 | 0x34 | 0x64 |
| | 8 | 0-7 | 0xC3 | 0x18 | 0x33 | 0x65 |
| | 9 | 0-7 | 0xC5 | 0x17 | 0x32 | 0x66 |
| | 10 | 0-7 | 0xC6 | 0x16 | 0x31 | 0x67 |
| | 11 | 0-7 | 0xC7 | 0x15 | 0x2E | 0x68 |
| | 12 | 0-7 | 0xC9 | 0x14 | 0x2D | 0x69 |
| | 13 | 0-7 | 0xCA | 0x13 | 0x2C | 0x6A |
| | 14 | 0-7 | 0xCB | 0x12 | 0x2B | 0x6B |
| | 15 | 0-7 | 0xCC | 0x11 | 0x2A | 0x6C |
| | 16 | 0-7 | 0xCD | 0x10 | 0x2(| 0x6D |
| | 17 | 0-7 | 0xCE | 0x0F | 0x27 | 0x6E |
| | 18 | 0-7 | 0xD1 | 0x0E | 0x26 | 0x6F |
| | 19 | 0-7 | 0xD2 | 0x0D | 0x25 | 0x70 |
| | 20 | 0-7 | 0xD3 | 0x0C | 0x23 | 0x71 |
| | 21 | 0-7 | 0xD4 | 0x0B | 0x1F | 0x72 |
| | 22 | 0-7 | 0xD5 | 0x0A | 0x1E | 0x73 |
| | 23 | 0-7 | 0xD6 | 0x09 | 0x1D | 0x74 |
| | 24 | 0-7 | 0xD9 | 0x08 | 0x1B | 0x75 |
| | 25 | 0-7 | 0xDA | 0x07 | 0x18 | 0x76 |
| | 26 | 0-7 | 0xDC | 0x06 | 0x17 | 0x77 |
| | 27 | 0-7 | 0xE0 | 0x05 | 0x10 | 0x78 |

continued

Table C-2
ALPA to SCSI Mapping *continued*

| Bus # | Target # | LUN # | *AL_PA | *SEL_ID | **AL_PA | **SEL_ID |
|-------------|----------|-------|--------|---------|---------|----------|
| 4 | 28 | 0-7 | 0xE1 | 0x04 | 0x0F | 0x79 |
| (continued) | 29 | 0-7 | 0xE2 | 0x03 | 0x08 | 0x7A |
| | 30 | 0-7 | 0xE4 | 0x02 | 0x04 | 0x7B |
| | 31 | 0-7 | None | None | None | None |
| 5 | 0 | 0-7 | 0xE8 | 0x01 | 0x02 | 0x7C |
| | 1 | 0-7 | 0xEF | 0x00 | 0x01 | 0x7D |
| | 2 | 0-7 | None | None | None | None |
| | 3 | 0-7 | None | None | None | None |
| | 4 | 0-7 | None | None | None | None |
| | 5 | 0-7 | None | None | None | None |
| | 6 | 0-7 | None | None | None | None |
| | 7 | 0-7 | None | None | None | None |
| | 8 | 0-7 | None | None | None | None |
| | 9 | 0-7 | None | None | None | None |
| | 10 | 0-7 | None | None | None | None |
| | 11 | 0-7 | None | None | None | None |
| | 12 | 0-7 | None | None | None | None |
| | 13 | 0-7 | None | None | None | None |
| | 14 | 0-7 | None | None | None | None |
| | 15 | 0-7 | None | None | None | None |
| | 16 | 0-7 | None | None | None | None |
| | 17 | 0-7 | None | None | None | None |
| | 18 | 0-7 | None | None | None | None |
| | 19 | 0-7 | None | None | None | None |
| | 20 | 0-7 | None | None | None | None |
| | 21 | 0-7 | None | None | None | None |

continued

Table C-2
ALPA to SCSI Mapping *continued*

| Bus # | Target # | LUN # | *AL_PA | *SEL_ID | **AL_PA | **SEL_ID |
|-------------|----------|-------|--------|---------|---------|----------|
| 5 | 22 | 0-7 | None | None | None | None |
| (continued) | 23 | 0-7 | None | None | None | None |
| | 24 | 0-7 | None | None | None | None |
| | 25 | 0-7 | None | None | None | None |
| | 26 | 0-7 | None | None | None | None |
| | 27 | 0-7 | None | None | None | None |
| | 28 | 0-7 | None | None | None | None |
| | 29 | 0-7 | None | None | None | None |
| | 30 | 0-7 | None | None | None | None |
| | 31 | 0-7 | None | None | None | None |

NOTE: Columns marked with a single asterisk (*) refer to the translation used with registry parameter ScanDown = 0. Columns marked with a double asterisks (**) refer to the translation used with registry parameter ScanDown = 1 (required for Secure Path)..

Index

A

- adapter cable (BN38-E-0B) 4-6
- Agent password 6-4
- ALPA to SCSI mapping 2-7, C-3
- ALPA valid settings C-1
- anti-thrash filter 1-3, 2-11
- Arbitrated Loop Physical Address *See* ALPA
- Auto-Failback 1-3

B

- bus number 2-4
- Bus/Target/LUN 6-9

C

- cabling and termination 4-5
- client software 5-3
- connection problems 6-5
- controller
 - I/O wind down 2-3
 - modified version 2-2
 - operational models 2-2
 - ownership 2-2
- controller serial number 6-9

D

- de-installing

- Secure Path Software B-1
- disk LUN UUID 6-9
- disk number 6-9
- display refresh 6-11
- drive letter 6-9
- Dual Cascaded Switch
 - configuration 2-8
- dual RAID controllers 1-2

E

- ESA10000/12000 2-2

F

- failback
 - anit-thrash filter 2-11
 - options 2-11
- failovers
 - controller 6-17
 - defined 2-10
 - path 6-16
 - policy 2-11
 - responding to events 6-17
- FC-AL path illustrated 2-6
- Fibre Channel
 - Dual-Switched Fabric 2-8
- Fibre Channel Arbitrated Loop
 - path 2-5
- Fibre Channel setup 3-1

H

- H8836-AA terminator 4-5
- host connections
 - lost connection icon 6-6
 - monitor illustrated 6-5
 - monitoring 6-5
 - responding to lost connection 6-6
- HszDisk defined 1-4

I

- icons
 - controller path failure 6-15
 - storage controller total path failure 6-16
 - storage system path failure 6-15
 - storage system total path failure 6-16
 - storageset failure 6-16
 - storageset total path failure 6-16
- installation
 - additional SCSI Host Bus Adapter 4-4
 - cabling and termination 4-5
 - client software 5-3
 - de-installing Secure Path software B-1
 - examine the existing single path 4-3
 - existing RA8000/ESA12000 configuration 3-7
 - Fibre Channel Secure Path 3-1
 - hardware verification 4-8
 - new RA8000/ESA12000 configuration 3-3
 - prepare existing RAID system 4-3
 - prepare new RAID system 4-3
 - RA8000/ESA12000 components 3-2
 - SCSI and One Windows NT Server 4-5

- SCSI cluster Hub
 - illustrated 4-7
- SCSI cluster Y-cable
 - illustrated 4-6
- SCSI pre-requisites 4-2
- SCSI Secure Path 4-1
- Secure Path server
 - software 5-2
- Windows NT cluster with SCSI Hubs 4-7
- Windows NT cluster with Y-Cables 4-6

K

- KGPSA Fibre Channel adapter 2-7

L

- load distribution
 - described 2-11
 - disabled 2-10
 - enabled 2-10
 - Microsoft Clusters 2-11
- login window 6-3
- LP6NDS35 mini-port driver 2-7
- LUN 2-4

M

- managing Secure Path 6-1
- manged entity 2-2
- Microsoft Cluster Server
 - environment 6-18
- multiple profiles 2-2
- multiple-bus mode 1-2

O

- Oracle Parallel Server
 - environment 6-19

P

- parallel SCSI-based configuration 2-3

- path definition 2-3
 - bus number 2-4
 - FC-AL illustrated 2-6
 - Fibre Channel Arbitrated Loop 2-5
 - LUN 2-4
 - management behavior 2-13
 - parallel SCSI 2-3
 - path status 2-9
 - port number 2-4
 - target ID 2-4
 - verification 2-12
- path management behavior
 - summary 2-13
- path states
 - active 2-9
 - available 2-10
 - failed 2-10
- path status
 - alternate paths 2-9
 - mode and state 2-9
 - preferred path 2-9
 - two offline modes 2-9
- path verification 1-3, 2-12
- physical path view 6-9
 - display refresh 6-11
 - polling interval 6-11
 - single host storage
 - profile 6-10
- polling interval 6-11
- port number 2-4
- PREFERRED_PATH unit
 - attribute 1-2
- profile limits 2-2
- profiles 2-2

R

- RA7000/8000 2-2
- RA8000/ESA12000
 - installation 3-3, 3-7
- RAID system preparation 4-3
- RaiDisk defined 1-4

S

- SCSI
 - cluster hub illustrated 4-7
 - Host Bus Adapter
 - preparation 4-4
 - installation prerequisites 4-2
 - one Windows NT server 4-5
 - path illustrated 2-5
 - paths described 2-4
 - Single Server illustrated 4-5
- Secure Path
 - Agent defined 1-4
 - auto-failback 1-3
 - load distribution 1-3
 - managed entities 2-2
 - manager defined 1-4
 - overview 1-1
 - path verification 1-3
 - profiles 2-2
 - setup defined 1-4
 - software components 1-4
 - technology 1-2
- Secure Path Environment
 - physical path view 6-9
 - RAID Array storage sets 6-9
 - Storage System View 6-8
 - Storage Systems and Controllers 6-8
 - system view window 6-8
- Secure Path Manager
 - about 6-1
 - changing Agent password 6-4
 - creating storage profile 6-4
 - defining storage files 6-2
 - editing storage profile 6-4
 - launching 6-2
 - login window 6-3
 - saving storage profile 6-3
 - selecting storage profile 6-4
 - setting Storage Profile
 - properties 6-7
 - system view window 6-8
 - using with MSCS and OPS
 - clusters 6-18
- server software 5-2

- SPM 6-1
- Storage Profile
 - creating 6-4
 - editing 6-4
 - saving 6-3
 - selecting 6-4
 - setting properties 6-7
- Storage System ID 6-8
- Storagesets
 - changing a preferred path 6-13
 - controller path failure 6-15
 - detecting failures 6-14
 - detecting path failures 6-15
 - making a path offline 6-13
 - making a path online 6-14
 - making a preferred path 6-13
 - making an alternate path 6-12
 - managing 6-12
 - moving 6-12
 - path failure icons 6-15
 - repairing a path 6-14
 - storageset path failure icon 6-16
 - total path failures 6-16
- SWCC
 - adding a system to the network 7-2
- T**
- target ID 2-4
- technical description of Secure Path 2-1
- terminators 4-5
- terminology for Secure Path A-1
- troubleshooting
 - client/agent considerations 8-2
 - connection problems 6-5
 - detecting path failures 6-15
 - detecting storageset failures 6-14
 - host connection monitor 6-5
 - identifying controller failovers 6-17
 - identifying path failovers 6-16
 - lost host connection icon 6-6
 - monitoring host connections 6-5
 - network considerations 8-2
 - path failure icons 6-15
 - responding to failover events 6-17
 - responding to lost host connection 6-6
 - total path failures 6-16
- U**
- Ultra SCSI cable (BN37A-05) 4-6
- uninstall Secure Path software *See* de-installing
- V**
- verification of paths 2-12
- verify hardware configuration 4-8
- VHDCI cables 4-7
- W**
- Windows filter driver *See* RaiDisk
- Windows NT class driver *See* HszDisk
- Windows NT cluster with SCSI Hubs 4-7
- Windows NT cluster with Y-cables 4-6
- Y**
- Y-cables 4-6