COMPAQ

StorageWorks Secure Path V2.0 for Sun Solaris

Installation and Reference Guide
AA-RKYDB-TE

Second Edition (January, 2000)
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.

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.

StorageWorks Secure Path V2.0 for Sun Solaris
Second Edition (January, 2000)
Part Number AA-RKYDB-TE

Contents

About This Guide

Chapter 1

Theory of Operation

Chapter 2

Technical Description

Chapter 3

Fibre Channel Secure Path Installation

Chapter 4
Installing Secure Path Software

Chapter 5
Managing StorageWorks Secure Path

Chapter 6
Troubleshooting

Appendix A
Glossary

Appendix B
Removing StorageWorks Secure Path Software

Appendix C
Valid ALPA Settings

List of Figures

List of Tables

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.

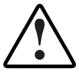
Text Conventions

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

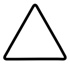
Keys	Keys appear in boldface. A plus sign (+) between two keys indicates that they should be pressed simultaneously.
USER INPUT	User input appears in a bold typeface and in lowercase.
FILENAMES	File names appear in uppercase italics.
Menu Options, Command Names, Dialog Box Names	These elements appear in initial capital letters.
COMMANDS, DIRECTORY NAMES, and DRIVE NAMES	These elements appear in uppercase.
Type	When you are instructed to *type* information, type the information **without** pressing the **Enter** key.
Enter	When you are instructed to *enter* 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.



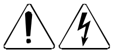
CAUTION: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.

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.

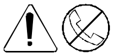
Symbols on Equipment

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 by logging on to the Internet 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 by logging on to the Internet 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

StorageWorks Secure Path is a high availability software product providing continuous data access for Fibre Channel RAID Array 8000 / Enterprise Storage Array 12000 storage systems configured on Sun Sparc platforms running Solaris 2.6 or Solaris 7 (**32-bit mode only**).

Redundant hardware, advanced RAID technology and automated failover capability are used to enhance fault tolerance and availability. Secure Path, in conjunction with the StorageWorks RAID system, eliminates the following as single points of failure: RAID controllers, disk drives, hubs, cables and host bus adapters.

Figure 1-1 illustrates a basic Secure Path hardware configuration. Note the physical connections that define the two separate paths, each originating at a separate host bus adapter on a Solaris server and ending at a port on a separate RAID controller on the storage system.

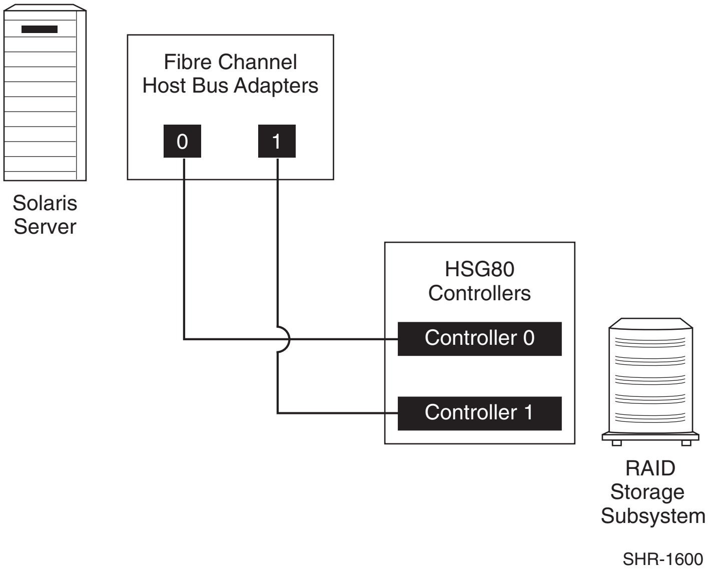


Figure 1-1. Basic Secure Path Configuration

Secure Path version 2.0 has the following features.

- Allows a StorageWorks dual-controller RAID system to be cabled on two independent Fibre Channel Arbitrated Loop paths using two host bus adapters (HBA) in each server.
- Monitors each path and automatically re-routes I/O to the functioning alternate path should an adapter, cable, hub or controller failure occur. Failure detection is reliable and designed to prevent false or unnecessary failovers. Failovers are transparent and non-disruptive to applications.
- Provides a Management Utility to monitor and manage Secure Path devices and paths.
- Provides support for Veritas Cluster Server high availability environments.

Secure Path Technology

The 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. During runtime, storage units may be moved between paths at any time using the Secure Path management utility.

The Secure Path software detects the failure of I/O operations on a failed path and automatically re-routes traffic to the other path. Path failover is completed seamlessly, without process disruption or data loss.

Following a warm-swap of an adapter or cable component, failed controller, or hub, storage units can be moved 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, or 3/5.

Chapter **2**

Technical Description

Overview

Secure Path is server-based software that enhances the StorageWorks RAID storage system by providing automatic recovery from server-to-storage system connection failures. Secure Path supports two I/O paths between a Solaris host and a RAID storage system, improving overall data availability. If any component in the path between the host and storage system fails, Secure Path redirects all pending and subsequent I/O requests from the failed path to the alternate path, preventing an adapter, cable or controller failure from disrupting data access.

Software Components

The Secure Path software consists of the Secure Path drivers (ldLite, mda and path), the spdaemon, and the spconfig, spmt and spinit management tools. Together, these software components are used to create, configure and manage redundant paths to a storage device. Figure 2-1 shows each component in the path along which data moves from an application to storage.

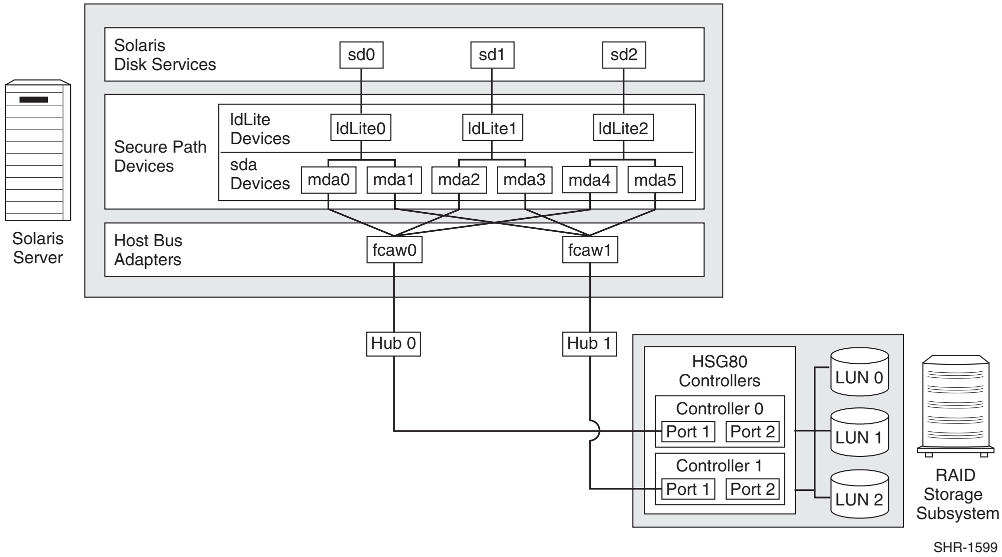


Figure 2-1. Software Components Comprising the Paths to Storage

Secure Path Drivers and spdaemon

The Secure Path (SP) drivers reside between the Solaris sd disk driver and the Fibre Channel (FC) host bus adapter driver. There are 3 drivers (mda, ldLite and path) that together along with the spdaemon provide Secure Path’s path failover functionality. When a path from the server to the storage system is active, the drivers act as a “pass-through” agent. All I/O from the Solaris sd driver is sent directly to the FC host bus adapter (HBA) driver.

When an active path fails (due to a cabling problem, for example), the mda driver stops sending I/O to the HBA driver and signals the Secure Path spdaemon that a failure event has been detected. The mda driver then activates the standby path and reissues all pending I/O as well as subsequent I/O to the newly active path. Once the standby path has successfully been activated, the driver signals the spdaemon that the failover has completed successfully. The spdaemon logs the event messages to the console and the system log file, and sends email notification to the root account on the host (or another specified user). The Secure Path drivers and the spdaemon are transparent to applications.

Secure Path Drivers

Secure Path consists of three drivers that together create and manage paths to a storage device while providing a single device target to applications. Figure 2-2 illustrates the driver model structure.

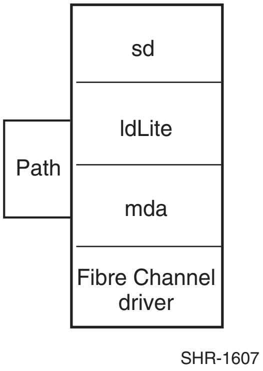


Figure 2-2. StorageWorks Secure Path V2.0 Driver Model

- **mda**

  The mda driver is a SCSI-disk target driver specific to the Compaq HSG80 fibre attached RAID storage system controller. The mda driver is a path failover driver which provides I/O paths to the storage devices. It also monitors the paths and, when a path failure is detected, automatically initiates path failover.

- **ldLite**

  The ldLite driver is a pseudo-HBA driver that presents separate mda instances as a single device to the Solaris sd driver.

- **path**

  The path driver provides facilities for the ldLite and mda drivers to communicate in the kernel. It also provides a character device interface that is used by the Secure Path management utility to manage the state of the paths to each storage device. The path driver is not used for any device I/O.

Failover

Secure Path redirects I/O from a failed physical path to the path still functioning. This process is known as path failover. If a problem with a host bus adapter, RAID controller, FC hub, or any connection hardware causes a path to fail, Secure Path stops sending I/O to the HBA driver, marks the path as failed, and assigns the standby path as the online path. After this reconfiguration, I/O is sent along the new online path. This failure-recovery process is transparent to applications.

Figure 2-3 shows a Secure Path environment on which a Solaris server has redundant connections to a RAID storage system.

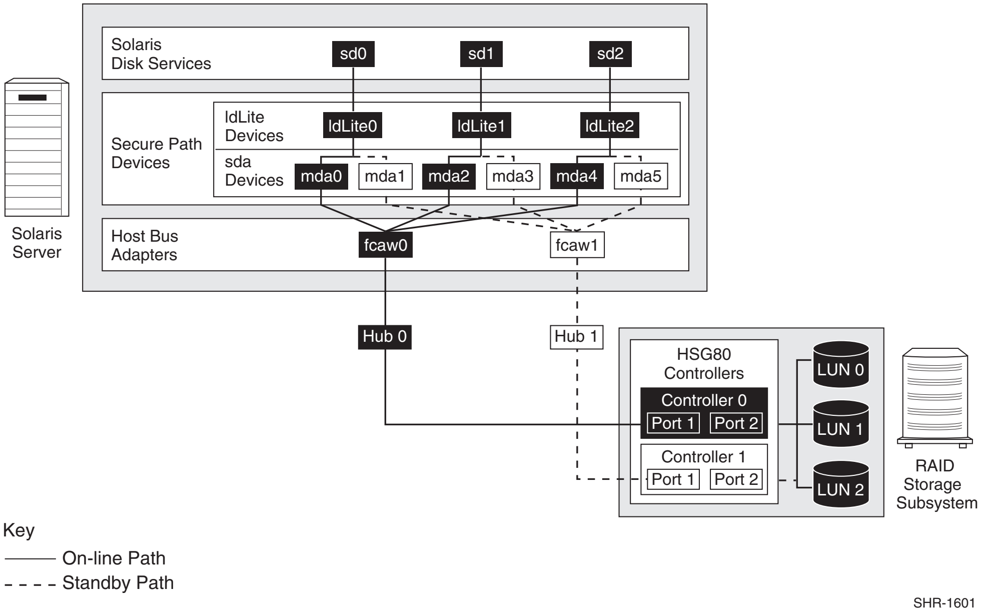


Figure 2-3. Before Path Failover

The RAID storage system has three LUNs and the Solaris server has 3 sd devices associated with the LUNs. Each device has 2 paths. The online path is shown in black and the standby in white. In Figure 2-3, the active path is shown as a solid line. The dashed line is the path that is on standby. (To clarify this example, each Secure Path device is accessing the LUN through the same HBA/FC hub/RAID controller. Normally, access to the LUNs would be balanced over both connections.)

As long as the online path is accessible, the Secure Path devices use this path for I/O. If the active path fails (due to a problem with the HBA fcaw0, for example), Secure Path detects the error and stops sending I/O along this path.

It then takes the path offline (marks it failed), brings the standby path online and redirects I/O to the newly active path as shown in Figure 2-4. The dotted lines denote the failed path.

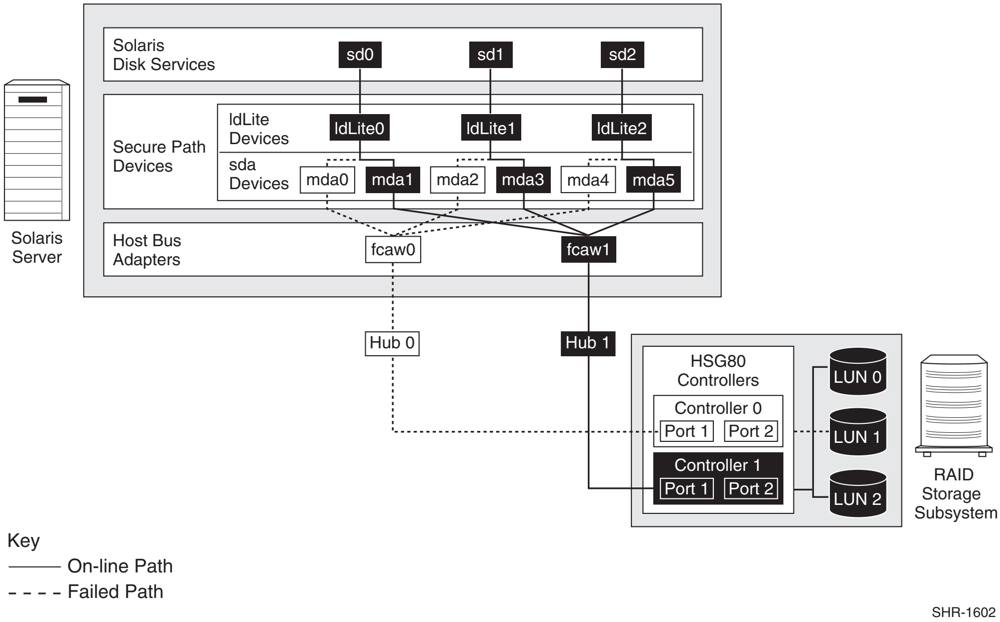


Figure 2-4. After Path Failover

Application Access

Applications access Secure Path devices by simply accessing the sd devices as they would normally. Each Secure Path device has a sd device instance associated with it and a corresponding c*X*t*Y*d*Z* device in /dev/dsk and /dev/rdsk directories.

Secure Path Device State

Each Secure Path device has a status that describes its current condition. The state of a Secure Path device is determined by the condition of its paths. The states for a device are as follows:

- **operational**

  An operational device has at least one physical I/O path open to a LUN on the storage system.

- **dead**

  A dead Secure Path device has no open physical I/O paths to the LUN. This device is out of service.

Secure Path Path State

The device path is the physical I/O path through which current I/O is moved between the host system and the LUN on the storage system. A Secure Path device path consists of a single FC host bus adapter, a FC hub, a single port on a RAID controller, and the associated cabling between the HBA and the FC hub and between the FC hub and the controller port.

A Secure Path device path has the following states:

- **online**

  The online state indicates that I/O is currently accessing this path.

- **standby**

  The standby state indicates that the path is being held in reserve against failure. If the online path fails, Secure Path brings the standby path into service as the online path.

- **quiesced**

  This path has been temporarily taken out of service to allow hardware maintenance, update and/or reconfiguration.

- **failed**

  The failed state indicates that Secure Path has closed this device path because of an underlying error. I/O will not be directed to this path.

Chapter **3**

Fibre Channel Secure Path Installation

To install a new Secure Path fibre channel configuration, or to build Secure Path onto an existing fibre channel configuration, it is recommended that you first refer to the RA8000/ESA12000 High Availability Application Notes for Sun Solaris found on the Compaq web site (see site address below). This will help you become familiar with the high availability connection layout (FC devices and cabling) of the configuration you want to install or add.

The application notes present a topological layout of several HA options; provide part numbers and reference documentation, and discuss restrictions that apply when Secure Path co-exists with Veritas Cluster Server software and FC hardware devices. At the time of this writing, the High Availability Application Notes document supporting Sun Solaris is as follows:

> RA8000/ESA12000 FC-AL High Availability Configurations for Sun Solaris

NOTE: For the most current Application Note information, please access the Compaq web page at:

www.compaq.com/products/storageworks

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

Verify that you have received the Secure Path software kit and the FC hardware ordered for your installation. If you are missing any component, please contact your 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	Sun Sparc
Operating System	Solaris 2.6; Solaris 7 (**32-bit mode only**)
Sun Hardware	▪ Sun4d Servers ▪ Sun4u Servers
Secure Path Software Kit	StorageWorks Secure Path v2.0 for Sun Solaris
RAID Storage System(s)	StorageWorks RA8000/ESA12000 (FC) with dual controllers
Solution Software Kit	StorageWorks Solution Software V8.5 for Sun Solaris
Host Bus Adapter(s) (and adapter driver)	Supported model for Sun Solaris: ▪ FC PCI 32-bit Adapter 380576-001 (SWSA4-PC) ▪ FC Sbus 64-bit Adapter 123503-001 (DS-SWSA4-SC)
FC Hub and Cables	▪ 7-port hub 242795-B21 (DS-SWXHX-07) ▪ 12-port hub 245573-B22 (DS-DHGGB-AB) ▪ FC Cables 234457-* (BNGBX-nn)

Installing and Configuring the RAID System for Secure Path

This section provides the steps for installing and configuring your RAID system(s) and Sun server(s) for Secure Path operation.

IMPORTANT: If this is an installation of Secure Path on an existing RAID storage system, **all** I/O to the RAID system must be stopped and steps 1 and 2 below, skipped.

1. Unpack your RAID system and install the PCMCIA cards in the controllers.

   NOTE: Secure Path V2.0 for Sun Solaris requires StorageWorks ACS version 8.5F software on the RAID storage system.

2. Power ON your RAID system. Allow the cache batteries to charge, if necessary, before proceeding.

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

3. Establish a serial connection to the RAID storage system and use the Command Line Interface (CLI) utility to configure the RAID system and create storagesets, as described in Chapter 3 of the *RA8000/ESA12000 HSG80 Solution Software V8.5 for Sun Solaris 2.x – Installation Reference Guide*.

   WARNING: Before proceeding, allow initialization of the storagesets to complete.

   NOTE: Secure Path installation requires that at least one LUN be configured on the RA8000/ESA12000 system, but a complete disk device configuration is recommended.

4. Using the Command Line Interface (CLI), determine the configuration of the RAID system with the following command:

   HSG80 > **show this_controller**

   or

   HSG80> **show other_controller**

   An example of the controller output follows: (line numbers appended for reference)

```
Controller:                                                              1.
    HSG80 ZG90305234 Software V85F-0, Hardware  E05                      2.
    NODE_ID          = 5000-1FE1-0000- 8920                              3.
    ALLOCATION_CLASS = 0                                                 4.
    SCSI_VERSION     = SCSI-2                                            5.
    Configured for dual-redundancy with ZG90811309                       6.
      In dual-redundant configuration                                    7.
    Device Port SCSI address 6                                           8.
    Time: NOT SET                                                        9.
    Command Console LUN is disabled                                     10.
Host PORT_1:                                                            11.
    Reported PORT_ID = 5000-1FE1-0000- 8921                             12.
    PORT_1_TOPOLOGY  = LOOP_HARD (standby)                              13.
    PORT_1_AL_PA     = 72 (72 negotiated)                               14.
Host PORT_2:                                                            15.
    Reported PORT_ID = 5000-1FE1-0000- 8922                             16.
    PORT_2_TOPOLOGY  = LOOP_HARD (loop up)                              17.
    PORT_2_AL_PA     = 71 (71 negotiated)                               18.
    NOREMOTE_COPY                                                       19.
Cache:                                                                  20.
    64 megabyte write cache, version 0012                               21.
    Cache is GOOD                                                       22.
    No unflushed data in cache                                          23.
    CACHE_FLUSH_TIMER = DEFAULT (10 seconds)                            24.
Mirrored Cache:                                                         25.
    64 megabyte write cache, version 0012                               26.
    Cache is GOOD                                                       27.
    No unflushed data in cache                                          28.
Battery:                                                                29.
    NOUPS                                                               30.
    FULLY CHARGED                                                       31.
    Expires:              16-DEC-2001                                   32.
```

a. If the controllers are in Transparent Failover Mode (see line 6 of example controller output) then they must be reconfigured for multiple-bus failover. Configure the RAID system controllers for multiple-bus failover mode, using the commands below.

```
HSG80> set nofailover

HSG80 > set multibus_failover copy = this_controller
```

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_controller
HSG80> show other_controller
```

Line 6 of the controller output should be similar to the following (ignoring the value of the serial number):

```
Configured for MULTIBUS_FAILOVER with ZG90811309
```

b. Set the Preferred Path for each storage unit to specify the controller that the unit will use upon the RAID system boot time as follows:

First, enter the following command to obtain a list of all units defined in the RAID system:

```
HSG80 > show units full
```

An example of the "show units" output follows:

```
D11                               DVGRPR0    (partition)
        LUN ID:     6000-1FE1-0000-8920-0009-9030-5234-006E
        NOIDENTIFIER
        Switches:
          RUN               NOWRITE_PROTECT       READ_CACHE
          READAHEAD_CACHE       WRITEBACK_CACHE
          MAXIMUM_CACHED_TRANSFER_SIZE = 32
        Access:
              ALL
        State:
          ONLINE to this controller
          Not reserved
          NOPREFERRED_PATH
        Size:          8533749 blocks
        Geometry (C/H/S): ( 1680 / 20 / 254 )
```

As shown in this example, the state of the path is on-line to this_controller and no preferred path has been assigned.

Next, enter the following commands to specify the preferred path for each of the units:

HSG80 > **set *(unit #)* preferred_path = this_controller**
- or -
HSG80 > **set *(unit #)* preferred_path = other_controller**

Example:

```
HSG80 > set d11 preferred_path = other_controller
```

To transition the units to the preferred path, enter the following CLI commands:

```
HSG80> shutdown other_controller

HSG80> shutdown this_controller
```

Depress the reset button on each controller at the same time.

5. Power down the server. Install the Fibre Channel adapters as necessary per the adapter installation instructions. Cable the Fibre Channel Adapter and the RAID storage system to the hubs, as shown in Figure 3-2.

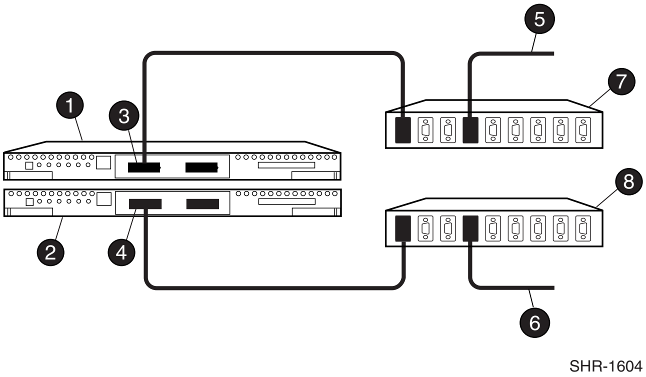


Figure 3-2. Cabling Two RAID Controllers and Two FC Hubs

❶	HSG80 Controller A	❺	FC cable to host bus adapter A
❷	HSG80 Controller B	❻	FC cable to host bus adapter B
❸	Controller 1, port 1 (to host via top hub)	❼	FC-AL hub (top)
❹	Controller 2, port 1 (to host via bottom hub)	❽	FC-AL hub (bottom)

6. Power on the server.
7. Boot the system using the reconfiguration switch as follows:

   For Solaris 2.6: ok> **boot -r**

   NOTE: Secure Path v2.0 for Sun Solaris is only supported in 32-bit kernel mode.

   For Solaris 2.7: ok> **boot kernel/unix -r**

   NOTE: Secure Path installation requires that at least one disk device with two paths is configured on the RA8000/ESA12000 system.

8. Install or reinstall the RA8000/ESA12000 Solution Software V8.5 for Solaris 2x and configure the fibre channel drivers for loop mode.

   NOTE: Refer to the *RA8000/ESA12000 HSG80 Solution Software V8.5 for Sun Solaris – Installation Reference Guide* for detailed Solution Software configuration information, including SWCC Agent and arbitrated loop.

9. Check to ensure that each connection has an offset of 0 and that its operating system is set to SUN, using the following commands:

   a. To inspect the connection settings, enter:

      HSG80 > **show connections**

      Example "show connections" output:

```
Connection                                                                Unit
Name         Operating system    Controller  Port    Address    Status   Offset

!NEWCON32          SUN              THIS       2      000001   OL this       0
           HOST_ID=1000-00E0-6940-123C         ADAPTER_ID=2000-00E0-6940-123C

!NEWCON34          SUN              OTHER      2      000001   OL other      0
           HOST_ID=1000-00E0-6940-11A8         ADAPTER_ID=2000-00E0-6940-11A8
```

   b. To set the operating system:

      HSG80 > **set (c*onnection name)* operating_system = sun**

   c. To set the offset, if necessary:

      HSG80 > **set (c*onnection name)* unit_offset = 0**

System is now ready for the installation of the Secure Path Software in Chapter 4.

Chapter 4

Installing Secure Path Software

Secure Path Pre-Installation Checklist

This section provides the procedures to install and configure Secure Path software. To proceed, the following requirements must be met:

- Sun server has StorageWorks Solution Software v8.5 for Sun Solaris installed
- RAID storage system(s) have StorageWorks ACS V8.5F firmware installed
- Successful completion of the FC Installation procedures in Chapter 3
- Only one physical connection (path) exists between each controller and each host bus adapter
- The RAID storage system(s) is configured with the desired storagesets. At least one LUN is configured on the RAID system and is visible to the server.

The Secure Path Configuration Tool

During the installation of the Secure Path software, the installation utility, spconfig is called to configure the Secure Path software for the target host system.

The spconfig utility is designed as a first-time, non-reentrant configuration utility for the files mda.conf, ldLite.conf and sd.conf, all located in `/kernel/drv`. It requires at least one LUN with two visible paths on the server. This LUN enables communication with the RAID storage system, gathering information required for the configuration files noted above.

Some configurations may present too many combinations for spconfig to determine the desired HBA and RAID storage system combination(s). In such cases, spconfig will make an attempt to configure, but if unsuccessful, will issue a message that it is unable to configure the specific configuration for Secure Path. Should this situation present itself, the spconfig utility must then be run interactively, requiring user input to define the configuration. Interactive configuration is achieved by invoking the spconfig with the operator switch (-o), as follows:

```
# /opt/CPQswsp/bin/spconfig -o -p /kernel/drv
```

At each prompt, provide input as required.

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

Installing Secure Path Software

1. Back up the entire system according to normal procedures.
2. Mount the CD-ROM.

   Check that the volume management daemon (vold) is currently running. Enter:

   ```
   # ps -ea l grep vold
   ```

   Follow the steps below for “vold currently running” or “vold not currently running,” as applicable:

If *vold* is currently running, then:

a. Insert the CD-ROM into the CD-ROM Drive.

b. Check that the volume manager has automatically mounted the CD-ROM, by entering:

```
# mount
```

NOTE: The system command may take a few seconds to mount the CD-ROM. If the *mount* command does not indicate that the CD-ROM has been mounted, wait a short interval and then repeat the command. The *volcheck* command may be used to force *vold* to check for mounted media.

c. Change to the Solaris directory. Enter:

```
# cd /cdrom/sp_v20_sun/solaris
```

d. Continue with step 3.

If *vold* is not currently running, then:

a. Insert the CD-ROM into the CD-ROM drive.

b. Mount the CD-ROM. For example, enter:

```
# mount –f hsfs –r /dev/dsk/c0t6d0s2 /cdrom
```

c. Change to the Solaris directory, enter:

```
# cd /cdrom/sp_v20_sun/solaris
```

d. Continue with step 3.

3. Install Secure Path software (CPQswsp) on the Sun Solaris server(s). The Secure Path software is installed using the Solaris “pkgadd” utility. Enter:

```
# pkgadd –d pkgs
```

NOTE: The following steps apply only after the Secure Path configuration utility has been run successfully, as described in the in the *Secure Path Configuration Tool* section of this chapter.

4. Reboot the server(s).

5. Verify the Secure Path configuration by running the Secure Path Maintenance Tool.

Example:

```
# /opt/ CPQswsp/bin/spmt display
```

```
Device: c2t0d0     Status: Operational

Storage System: 5000-1fe1-0000-8920
LUN: 6000-1fe1-0000-8920-0009-9030-5234-005a
==========================================================
Controller   Unit   State     HBA       Path
==========================================================
ZG90811309   D0     standby   fcaw0     /sbus@3,0/fcaw@0,0
ZG90305234   D0     online    fcaw1     /sbus@b,0/fcaw@0,0
```

The initial installation for Secure Path v2.0 will configure the existing RAID system(s), making all LUNs available to the host server.

Adding and Deleting Units to the RAID System

In a production environment, however, the configuration may have to be changed with the addition or removal of a LUN at the RAID Array. For these configuration changes, the following steps must be taken to allow the server to acquire the new Target/LUN combinations.

NOTE: These steps assume that no I/O is being sent to the RAID storage system.

Adding a Unit

The steps to adding a Unit to a Secure Path installation are as follows:

1. Add the Unit to the RAID Array using the CLI or SWCC interface.

   Example:

   ```
   HSG80> add unit D18 S1
   ```

2. Initialize the new Unit.

   Example:

   ```
   HSG80> initialize D18
   ```

3. Display the Unit’s LUN ID. Enter:

   ```
   HSG80> show unit full
   ```

   The LUN ID is displayed in the hex format: *nnnn-nnnn-nnnn-nnnn-nnnn-nnnn-nnnn-nnnn*. Record this value.

Example:

```
LUN ID:     6000-1FE1-0000-8920-0009-9030-5234-006E
```

4. On the server, in the `/kernel/drv` directory, edit the following three files as described:

   a. **mda.conf** – add two new path entries to the host Target. (Chapter 6 explains the path entries).

   Example:

   ```
   name="mda" parent= "/sbus@3,0/fcaw@0,0" target=64 lun=18;
   name="mda" parent= "/sbus@b,0/fcaw@0,0" target=64 lun=18;
   ```

   b. **ldLite.conf** – add the new LUN ID, recorded in Step 3.

   Example:

   ```
   targ18-devName = "6000-1FE1-000-0D40-0090-8090-0656-0123";
   ```

   c. **sd.conf** – verify that an entry exists to map to the new entry added to the mda.conf file. Thus, if there are now 18 Target/LUN combinations, an entry in sd.conf must be added to map that Target.

   Example:

   ```
   name="sd" class = "scsi"  target = 18, lun=0;
   ```

5. Reboot the server, by entering:

   ```
   # reboot -- -r
   ```

6. Verify that the server has acquired the new UNIT. Enter:

   ```
   # format
   ```

Deleting a Unit

1. On the RAID system, using the CLI or the SWCC display, identify the UNIT to be removed using the following command:

   ```
   HSG80> show units full
   ```

   The LUN ID assigned to that UNIT is displayed in the hex format: *nnnn-nnnn-nnnn-nnnn-nnnn-nnnn-nnnn-nnnn.* Record this value.

   Example:

   ```
   LUN ID:    6000-1FE1-0000-8920-0009-9030-5234-006E
   ```

2. Delete the UNIT using the CLI or SWCC interface.

   Example: `HSG80> delete D18`

3. On the server, in the `/kernel/drv` directory, edit the following three files as described:

   a. **mda.conf** – delete the two path entries to the host Target. (Chapter 6 explains the path entries).

      Example:

      name="mda" parent= "/sbus@3,0/fcaw@0,0" target=64 lun=18;
      name="mda" parent= "/sbus@b,0/fcaw@0,0" target=64 lun=18;

   b. **ldLite.conf** – delete the LUN ID, recorded in Step 1.

      Example:

      targ18-devName = "6000-1FE1-000-0D40-0090-8090-0656-0123";

   c. **sd.conf** – examine this file to see **if** an entry was added to it, If so, delete the entry. By default, the sd.conf file has 16 entries (minus the entry for target 7, reserved for the SCSI initiator).

      Example: name="sd" class = "scsi" target = 18, lun=0;

4. Reboot the server by entering the following command:

   ```
   # reboot -- -r
   ```

5. Verify that the server has deleted the UNIT. Enter:

   ```
   # format
   ```

Chapter 5

Managing StorageWorks Secure Path

Managing a Secure Path Environment

Secure Path provides two utilities to manage a Secure Path environment. These two utilities are spmt and spinit. The spmt manages paths, displays status and permits CLI access to the controller. The spinit manages the spdeamon that detects path events and sends email notification to a specified mail address.

Secure Path Management Tool (spmt)

Table 5-1 lists the command options for spmt. Each option is described on the following pages.

Table 5-1
spmt Command Options

Commands	Action(s)
display	Displays status and information about Secure Path devices.
cli	Invokes a command line interpreter (CLI) session to the RAID controller.
toggle	Switches the I/O to the standby path.
restart	Sends a CLI RESTART command to a specified controller.
shutdown	Sends a CLI SHUTDOWN command to a specified controller.
restore	Restores a Secure Path device to its preferred path.
remove	Quiesces paths for a specified HBA.
reconfig	Activates paths for a specific HBA.

spmt Commands

spmt display

The **spmt display** command displays information about Secure Path devices, including the controllers, paths, and host bus adapters used by that Secure Path device.

The **spmt display** command has the form:

```
# spmt display -t  target_number
```

where:

Default displays information and status for all Secure Path devices.

target_number is the Secure Path target assigned to the storage unit.

Example:

```
# spmt display –t 9
```

```
Device: c3t9d0     Status: Operational

Storage System: 5000-1fe1-0001-ed20
LUN: 6000-1fe1-0001-ed20-0009-9281-0158-0005
==========================================================
Controller  Unit  State     HBA       Path
==========================================================
ZG92810158  D110  online   fcaw0     /sbus@49,0/fcaw@1,0
ZG92810434  D110  standby  fcaw1     /sbus@50,0/fcaw@1,0
```

Each field in the output is described in Table 5-2

Table 5-2
Fields Displayed by "spmt display"

Field	**Value**	**Meaning**
Device (File)	CXtYdZ	The Secure Path device
Status (of device)	operational dead	The Secure Path device can be accessed on at least one path. All device paths used by this Secure Path device have failed.
Storage System	WWNN	Fibre Channel World Wide Node Name assigned to the RAID storage system
LUN	WWID	Fibre Channel World Wide LUN identifier
Controller	10 character alphanumeric	Serial number of the RAID controller
Unit	D*n*	Unit number that the storage RAID system.
State (of Path)	online standby failed quiesced	Active path for the Secure Path device Alternate path for the Secure Path device Path is unavailable for I/O Path disabled for I/O by the user
HBA	Adapter instance number	Identifies the host bus adapter
Path (hardware)	HBA hardware parent string	The string that represents the complete hardware path of bus and instance of the adapter.

spmt cli

The **spmt cli** command invokes a CLI session with a RAID controller. **spmt** opens a session with the RAID controller on the active path of the specified Secure Path device.

The **spmt cli** command has the form:

```
# spmt cli -t  target_number
```

where:

Default = open the cli to the first online path

***target_number* =** the Secure Path target assigned to the storage unit

Example:

```
# spmt cli -t 2

HSG80>
```

NOTE: To end the CLI session, type **q**

WARNING: This CLI session does not support the run command for the controller utilities.

spmt toggle

The **spmt toggle** command changes the path that a Secure Path device uses to access a LUN. The online path becomes the standby path, the standby path becomes the online path. Use this command to manually distribute LUN access across different paths, for better performance.

NOTE: In a multi-host environment, toggle will only move LUNs that are currently available on the local host.

The **spmt toggle** command has the form:

```
# spmt toggle -t  target_number
```

where:

target_number is the Secure Path target assigned to the storage unit.

Example:

```
# spmt toggle –t 2
```

spmt restart/spmt shutdown

The **spmt restart** and **spmt shutdown** commands cause I/O to be redirected to the other controller. The **spmt restart** command will function if multiple hosts are actively accessing LUNs. Therefore, if Secure Path is active on those hosts, I/O will be properly transferred to alternate paths.

The difference between **restart** and **shutdown** is that restart will cause the controller to reboot, while shutdown will stop the controller.

The purpose of these two commands is to move all online LUNs from the specified controller to the other controller. This allows the user to perform maintenance operations on the specified controller.

These commands have the form:

# spmt restart -c *serial_number*

# spmt shutdown -c *serial_number*

where:

> ***serial_number*** specifies the RAID controller to be taken offline.

Examples:

```
# spmt restart –c ZG92810158
# spmt shutdown –c ZG92810158
```

### spmt remove

The **spmt remove** command quiecses the path for a specified host adapter adapter. All I/O is redirected to the other path and the removed path is marked quiesced. This also disables the path for future I/O until a **spmt reconfig** is issued.

The **spmt remove** command has the form:

# spmt remove -a *hba*

where:

> ***hba*** refers to the instance of the Solaris host bus adapter

(for example, fcaw0). You can obtain this value from the HBA field in the table generated by **spmt display**.

Example:

```
# spmt remove -a fcaw1
```

spmt reconfig

The **spmt reconfig** command restores the host bus adapter path that was removed from the Secure Path configuration by the **spmt remove** command. The **spmt reconfig** does not restore path usage to PREFERRED_PATH.

You must use the **spmt restore** command to re-establish PREFERRED_PATH usage.

The **spmt reconfig** command has the form:

```
# spmt reconfig -a hba
```

where: ***hba*** refers to the instance of the Solaris host bus adapter

Example:

```
# spmt reconfig –a fcaw1
```

Secure Path daemon tool (spinit)

spinit

The s**pinit** utility to start and stop the Secure Path **spdaemon**.

The **spinit** utility has the form:

```
# spinit start [email_address]

# spinit stop
```

where: **start** starts the **spdaemon**

stop stops the **spdaemon**

email_address specifies where to send mail when an event takes place that may require action. The default is the root account on the server.

Chapter 6

Troubleshooting

This chapter lists the configuration files, file entries, and specific formats for entries, required for proper Secure Path operation.

Configuration Files

Table 6-1 lists the files modified as part of the Secure Path V2.0 installation.

Table 6-1
Modified Configuration Files

Files	Description
/etc/driver_classes	Registers the ldLite driver
/etc/devlink.tab	Defines devlinks entry for the ldLite
/kernel/drv/sd.conf	Modifies sd entries for Secure Path devices

Table 6-2 lists the files added as part of the Secure Path V2.0 installation:

Table 6-2
Files Added by Secure Path V2.0

Files	Description
/kernel/drv/mda.conf	Configuration file for the mda driver
/kernel/drv/ldlite.conf	Configuration file for ldLite driver

/etc/driver_classes

In order for the ldLite driver to be properly associated with a driver class the following entry has been added to the driver_classes file:

```
ldLite  scsi
```

/etc/devlink.tab

In order that Secure Path utilities communicate to the drivers, devlink.tab must include the following entry:

```
type=ddi_pseudo;name=ldLite;minor=ctl   pathCtl
```

/kernel/drv/sd.conf

All Secure Path devices must have a corresponding sd target entry. The default sd.conf file already has targets 0-15 defined (except target 7, which is reserved for the adapter). For example, Secure Path device target 20 would have the following entry:

```
name="sd" class="scsi" target=20 LUN=0;
```

/kernel/drv/mda.conf

Secure Path device paths are configured by the mda driver utilizing the entries of the mda.conf file. The entries designate the hardware path, the controller target (AL_PA), and the LUN assignment.

```
name="mda" parent="/sbus@49,0/fcaw@1,0" target=65 LUN=20 qdepth=32;

name="mda" parent="/sbus@50,0/fcaw@1,0" target=64 LUN=20 qdepth=32;
```

/kernel/drv/ldLite.conf

Secure Path device files are configured by the ldLite driver utilizing the ldLite.conf file. The entries designate the specific units identified by the World Wide LUN Id as assigned by the RAID system. For every LUN assignment in mda.conf there is matching targ*n*-devName (/dev/rdsk/cXtYdZ) in ldLite.conf.

Additionally the first entry assigns a driver (ldLite) with a pseudo hardware path for a SCSI class.

```
name="ldLite" parent="pseudo" class="scsi" instance=0;

targ0-devName="6000-1FE1-0001-ED10-0009-9281-0311-0001";

targ1-devName="6000-1FE1-0001-ED10-0009-9281-0311-0002";
```

For further assistance, refer to the Compaq website or hotline in the *Getting Help* section at the front of this guide.

Appendix A

Glossary

StorageWorks Secure Path Terminology

Controller The hardware device that facilitates communication between a host and one or more LUNs organized as an array. Secure Path supports the HSG80 array controller. Each controller in a HSG80 RAID system is identified by a unique World Wide ID.

HBA The I/O device (Host Bus Adapter) which serves as the interface connecting a host system to the SAN (Storage Area Network).

Host The computer system on which the Secure Path server software is running.

LUN The LUN is the actual unit number assigned to a device at the RAID system controller.

Path A communication route that enables data and commands to pass between a host server and a storage device.

State Attributes that describe the current operational condition of a path. A path may exist in the following state(s):

- **online** indicates a path that is currently servicing I/O requests.
- **failed** - a path that is nonfunctional and not actively servicing I/O requests.

- **standby** - a path that is neither online nor failed. It is available to receive I/O if an alternate path fails.
- **quiesced -** the path has been disabled by the user.

Status Attributes that describe the current operational condition of a device. A device may exist in the following state(s):

- **operational -** the Secure Path device can be accessed on at least one path.
- **dead -** all paths used by this Secure Path device have failed.

Target For Fibre Channel configurations, the target number is assigned by a mapping function at the driver level and is derived from AL_PA (Arbitrated Loop Physical Addresses) in a FC-AL topology.

Appendix B

Removing StorageWorks Secure Path Software

This appendix describes how to remove StorageWorks Secure Path software from your server. Removing the Secure Path software will restore the server to a single path, RAID storage environment.

Under a single path configuration, the controllers must be set in a (Transparent) Failover mode. The steps to accomplish the removal of the software and the transition of the HSG80 controllers to (Transparent) Failover mode are described below.

How to Remove StorageWorks Secure Path Software

Removing the Software

1. On the specific server(s), invoke the Sun Solaris package remove function and select CPQswsp as shown below:

```
# pkgrm CPQswsp
```

2. When the Secure Path package has been removed, visit the area `/opt/steam/bin` (the default area), or the area selected during the installation of the HSG80 package, and invoke the following:

   ```
   # ./config.sh
   ```

   During the installation of the Secure Path software, target entries are removed from the `/kernel/drv/sd.conf` file and moved to the mda.conf and ldLite.conf files.

   The following steps regenerate the sd.conf file for use with the fibre channel drivers as a single path application. During these steps, new target names and new LUN values may be chosen.

   a. Using the Option 20, Add/Change Adapters, select each adapter and reselect the mode of operation, the desired targets, the desired number of LUNS and the specific World Wide Port Names for the intended RAID array.

   b. Press RETURN to complete each adapter update and the changes will be made to the `/kernel/drv/sd.conf` as well as the fibre channel driver configuration file(s), fca-pci.conf and/or fcaw.conf.

3. Reboot the server with the reconfigure switch, as follows:

   ```
   # reboot -- -r
   ```

   NOTE: If the same server and the same RAID storage system are to be reconnected, reconfigure the controllers on the RAID system using the steps below. After the controllers have been restarted, reboot the server as instructed above.

Reconfiguring the RAID Controllers

If the RAID storage system is to be used for single path access by one or more servers, then the HSG80 dual-redundant controllers must be placed in the Failover Mode known as Transparent Failover Mode.

The following steps will accomplish this change of controller state.

1. Establish a serial connection to the storage system.

2. If there are connections on the storage system, enter the following command:

   ```
   HSG80> show connections
   ```

Then, delete all connections, using:

```
HSG80>  delete connection_name  for each connection.
```

NOTE: The connections will be generated later.

3. If there are units (D*n*) on the storage system, they must be deleted. This is due to the inconsistencies incorporated in the volumes' WWID in different failover modes. Delete the units using the following commands:

```
HSG80> show units
```

```
HSG80> delete Dn
```

Repeat this step for each D*n* on the storage system.

NOTE: The Units will be restored after the controller state is changed. It is advised that the D*n* values and associated information and the storageset information be recorded for later use. The controller state change will not affect the data on the storagesets.

4. If the controllers are currently in a failover mode, enter:

```
HSG80> set nofailover
```

This command will cause the OTHER_CONTROLLER to shutdown. Restart the OTHER_CONTROLLER by pressing the RESET button on the OTHER_CONTROLLER.

The OTHER_CONTROLLER will sound an alarm as it discovers the second controller, but identifies that it is not bound in a failover mode. The alarm, which may be silenced, and the message about the controllers being misconfigured, may be disregarded.

5. When the OTHER_CONTROLLER is available, enter:

```
HSG80> set failover copy = this_controller
```

This action will restart the OTHER_CONTROLLER and copy all unit and configuration information to it. When restarted, the controller pair will be bound in Transparent Failover Mode. This change can be verified as follows:

```
HSG80> show this_controller
```

```
HSG80> show other_controller
```

6. Restore the UNIT to storage set mapping that was recorded earlier. Enter:

```
HSG80> add unit Dn storage_set_name
```

7. Restart both controllers so that connections may be reacquired.

```
HSG80> restart other_controller
HSG80> restart this_controller
```

NOTE: An alternative method to re-establish the connections is to reboot the server.

At this point, the server and RAID storage system are available for use with the single path, fibre channel applications.

Appendix C

Valid ALPA Settings

About ALPA Settings

Table C-1 lists the Arbitrated Loop Physical Address settings and corresponding SCSI target numbers for hard addressing the fibre channel arbitrated loop using the CPQfca-pci or CPQfcaw drivers. Use this table when setting the PORT_1_AL_PA and PORT_2_AL_PA addresses on the HSG80 controller. The default setting for port 1 is AL_PA=71 and port 2 is AL_PA=72. If you are configuring multiple HSG80 controllers on a loop, ensure that all ports on a loop have unique AL_PAs.

Table C-1
ALPA Settings

Host Server ALPAs **(Lowest to Highest Priority)**			**Controller Port ALPAs** **(Lowest to Highest Priority)**		
ALPA (hex)	Target (hex)	Target (dec)	ALPA (hex)	Target (hex)	Target (dec)
6E	42	66	EF	00	0
6D	43	67	E8	01	1
6C	44	68	E4	02	2
6B	45	69	E2	03	3
6A	46	70	E1	04	4
69	47	71	E0	05	5
67	48	72	DC	06	6
66	49	73	DA	07	7
65	4A	74	D9	08	8
63	4B	75	D6	09	9
5C	4C	76	D5	0A	10
5A	4D	77	D4	0B	11
59	4E	78	D3	0C	12
56	4F	79	D2	0D	13
55	50	80	D1	0E	14
54	51	81	CE	0F	15
53	52	82	CD	10	16
52	53	83	CC	11	17
51	54	84	CB	12	18
4E	55	85	CA	13	19
4D	56	86	C9	14	20
4C	57	87	C7	15	21
4B	58	88	C6	16	22
4A	59	89	C5	17	23
49	5A	90	C3	18	24
47	5B	91	BC	10	25
46	5C	92	BA	1A	26
45	5D	93	B9	1B	27
43	5E	94	B6	1C	28
3C	5F	95	B5	1D	29
3A	60	96	B4	1E	30
39	61	97	B3	1F	31
36	62	98	B2	20	32
35	63	99	B1	21	33
34	64	100	AE	22	34

continued

Table C-1
ALPA Settings *continued*

Host Server ALPAs **(Lowest to Highest Priority)**			**Controller Port ALPAs** **(Lowest to Highest Priority)**		
33	65	101	AD	23	35
32	66	102	AC	24	36
31	67	103	AB	25	37
2E	68	104	AA	26	38
2D	69	105	A9	27	39
2C	6A	106	A7	28	40
2B	6B	107	A6	29	41
2A	6C	108	A5	2A	42
29	6D	109	A3	2B	43
27	6E	110	9F	2C	44
26	6F	111	9E	2D	45
25	70	112	9D	2E	46
23	71	113	9B	2F	47
1F	72	114	98	30	48
1E	73	115	97	31	49
1D	74	116	90	32	50
1B	75	117	8F	33	51
18	76	118	88	34	52
17	77	119	84	35	53
10	78	120	82	36	54
0F	79	121	81	37	55
08	7A	122	80	38	56
04	7B	123	7C	39	57
02	7C	124	7A	3A	58
01	7D	125	79	3B	59
			76	3C	60
Reserved for Host Server FL_PORT:			75	3D	61
00	7E	126	***74***	***3E***	***62***
			73	***3F***	***63***
			72	***40***	***64***
			71	***41***	***65***

Note: *The gray area denotes addresses that are reserved for host bus adapters (not be used by HSG80 controllers). The most commonly used controller port ALPA addresses are in bold font.*