COMPAQ

SANworks Secure Path V2.1 for Sun Solaris
Installation and Reference Guide

Notice

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

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.

StorageWorks, SANworks, Neoserver, Netelligent, Systempro/XL, SoftPaq, QuickBlank, QuickLock are trademarks and/or service marks of Compaq Computer Corporation.

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.

Contents

Chapter 4
Installing Secure Path Software

Chapter 5
Managing SANworks Secure Path

Chapter 6
Troubleshooting

Appendix A
Glossary

Appendix B
Secure Path Configuration Upgrades

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:

user input	User input appears in a bold typeface and in lowercase.
paths/filenames	Directory paths and file names appear in narrow, lowercase letters (they are bold when part of a user command).
Menu Options	Menu options appear italicized and in initial capital letters.
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[1]. This service is available 24 hours a day, 7 days a week.

---

[1] 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

■ Detailed, specific questions

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

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

Redundant hardware, advanced RAID technology and automatic failover capability are used to enhance fault tolerance and availability. Secure Path, in conjunction with the StorageWorks RAID system, eliminates single points of failure such as RAID controllers, disk drives, FC hub or SAN switch, cables and host bus adapters.

Figure 1-1 illustrates a basic Secure Path hardware configuration. The physical connections define two separate paths. Each path originates at a unique host bus adapter on a Solaris server and ends at a port on a separate RAID controller on the storage system.
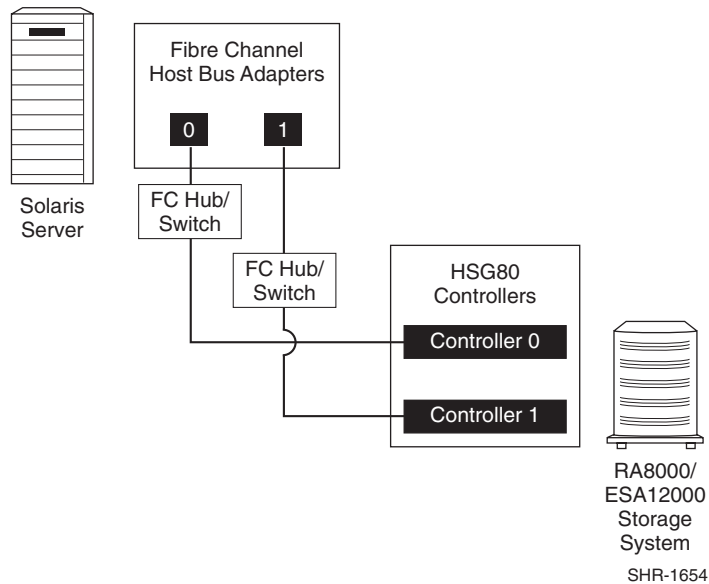
Figure 1-1. Basic Secure Path Configuration

Secure Path version 2.1 has the following features.

- Allows a StorageWorks dual-controller RAID system to be cabled on two independent Fibre Channel Arbitrated Loop (FC-AL) or switched fabric 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, FC hub or SAN switch, 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 tool to monitor and manage Secure Path devices and paths.

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. I/O is active to a specific LUN on a single controller at any time. During runtime, storage units may be moved (toggled) between paths at any time using the Secure Path management tool.

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, FC hub or SAN switch, storage units can be moved back to their original path using the Secure Path management tool.

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

SANworks 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, FC hub or SAN switch or controller failure from disrupting data access.

Software Components

The Secure Path software includes the following:

- drivers (ldLite, mda and path)

- spdaemon

- management tools (spconfig, spmt and spinit).

Secure Path uses these components 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.
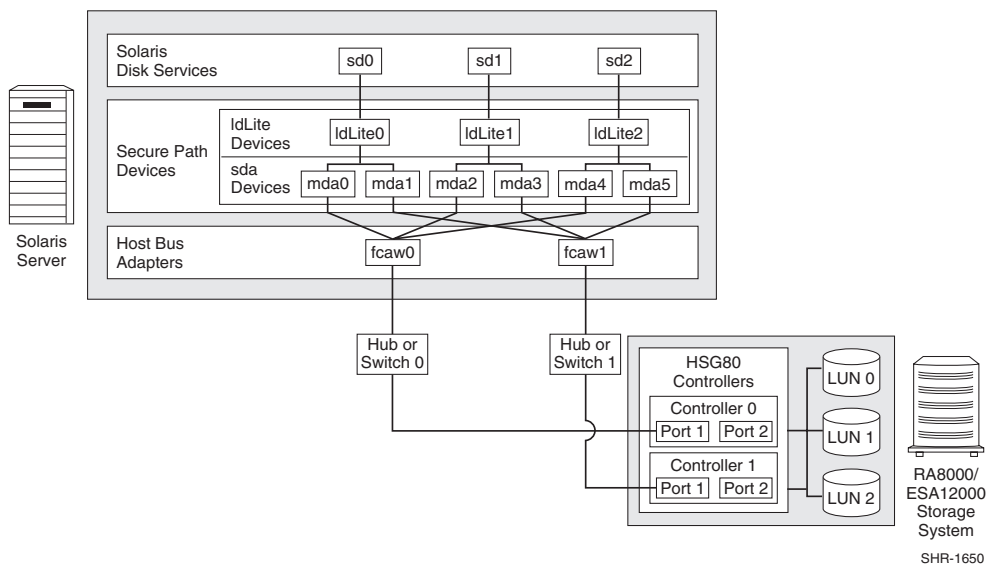
Figure 2-1. Software Components Comprising the Paths to Storage

Secure Path Drivers and spdaemon

Three Secure Path (SP) drivers (mda, ldLite and path) reside between the Solaris sd driver and the Fibre Channel (FC) host bus adapter (HBA) driver. These drivers, 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

The Secure Path drivers create and manage paths to a storage device while providing a single device target to applications. Figure 2-2 illustrates the driver model structure.
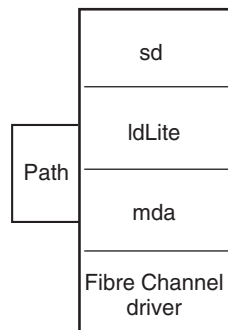
```
              ┌──────────────────┐
              │        sd        │
              │                  │
         ┌────┼──────────────────┤
         │    │      ldLite      │
         │Path│                  │
         │    ├──────────────────┤
         └────┼──────────────────┤
              │       mda        │
              │                  │
              ├──────────────────┤
              │  Fibre Channel   │
              │     driver       │
              └──────────────────┘
                  SHR-1607
```

Figure 2-2. SANworks Secure Path V2.1 Driver Model

■ **mda**

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

Path failover occurs when Secure Path redirects I/O from a failed physical path to the path still functioning. If a problem with a HBA, RAID controller, FC hub or SAN switch, 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.
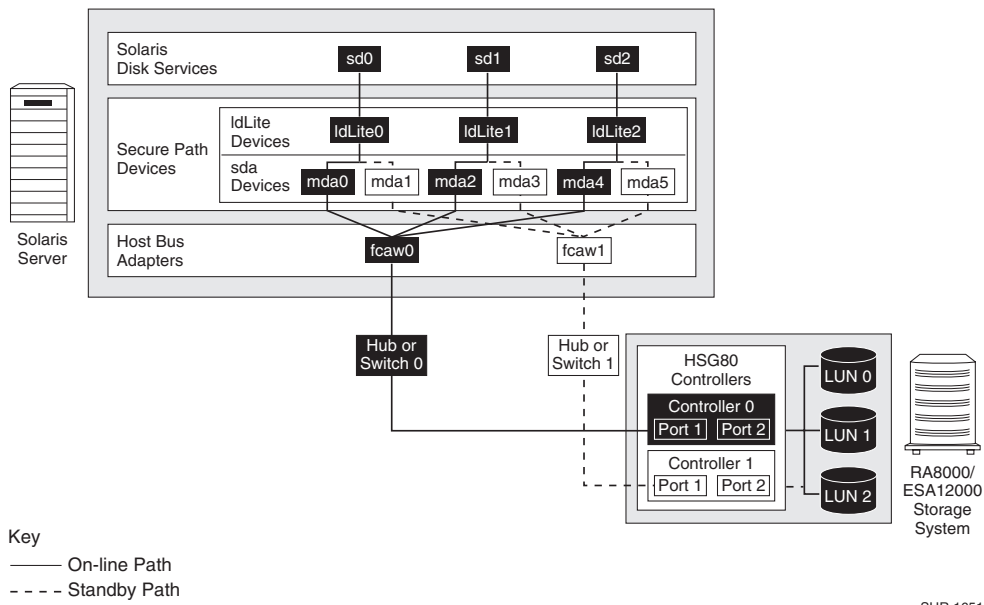
Figure 2-3. Before Path Failover

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. (Each Secure Path device is accessing the LUN through the same HBA-FC hub/SAN switch-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.
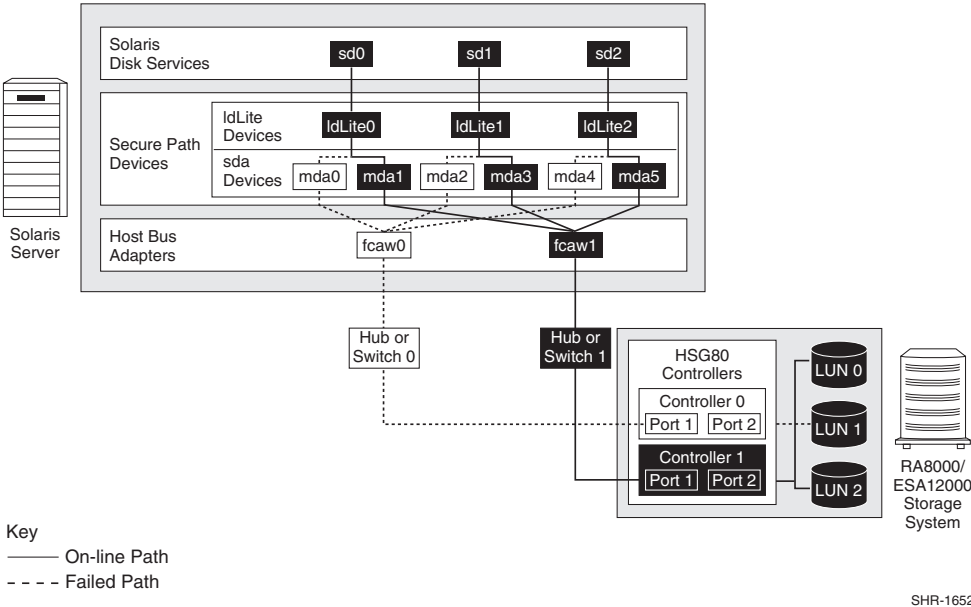
Figure 2-4. After Path Failover

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 States

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 Secure Path device are as follows:

■ **operational**

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

■ **dead**

The device has no open physical I/O paths to the LUN. This device is out of service.

Secure Path Device Path States

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 HBA, an FC hub or SAN switch, a single port on a RAID controller, and the associated cabling between the HBA and the FC hub or SAN switch, and between the FC hub or SAN switch and the controller port.

A Secure Path device path has the following states:

■ **online**

Indicates that I/O is currently using this path

■ **standby**

Indicates that the path is being held in reserve. If the online path fails, Secure Path brings the standby path into service.

■ **quiesced**

Indicates that the path has been taken out of service.

■ **failed**

Indicates that the path is no longer available for I/O.

Chapter **3**

Hardware Setup

This chapter provides the following FC Secure Path installation information:

■ Reference material for high availability connection options

■ Installation prerequisites

■ Installation procedures for hub-based FC Arbitrated Loop (FC-AL) mode

■ Installation procedures for switch-based FC Fabric (FC-SW) mode

High Availability Connection Options Reference Material

Before installing Secure Path on a new or existing Fibre Channel configuration, review the RA8000/ESA12000 High Availability Application Notes for Sun Solaris found on the Compaq web site. They will help familiarize you with the high availability connection layout (FC devices and cabling) of the configurations desired.

The application notes present a topological layout of several HA options. They also provide part numbers, list related product documents, and discuss restrictions that apply when Secure Path co-exists with VERITAS Cluster Server software and FC hardware devices. The High Availability Application Notes documents supporting Sun Solaris are:

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

b)   RA8000/ESA12000 Storage Area Network High Availability Configurations for Sun Solaris*

* contains FC Fabric configuration options

Access 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 any components are missing, 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	Sun Sparc
Operating System	Solaris 2.6; Solaris 7 (**32-bit mode only**)
Sun Hardware	▪ Sun4d Servers ▪ Sun4u Servers
Secure Path Software Kit	SANworks Secure Path V2.1 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

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

Host Feature	Requirement
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)

SAN Switches	Ports	Color	Part number	Supported Firmware*
	8	Blue	380591-B21 / DS-DSGGA-AA	V1.6d
	8	Opal	380591-B22 / DS-DSGGA-AC	V1.6d
	16	Blue	380578-B21 / DS-DSGGA-AB	V1.6d
	16	Opal	380578-B21 / DS-DSGGA-AD	V1.6d
	8	Blue	158222-B21 / DS-DSGGA-AA	V2.0.3a
	8	Opal	158223-B22 / DS-DSGGA-AC	V2.0.3a
	16	Blue	158224-B21 / DS-DSGGA-AB	V2.0.3a
	16	Opal	158225-B21 / DS-DSGGA-AD	V2.0.3a

* If the switch does not have the supported firmware, follow the instructions contained on the CD-ROM for the Sun Solaris Secure Path V2.1 release, found in: **cdrom/sp_v21_sun/firmware/README**.

GBICs	
	▪ FC Optical GBIC 380561-B21 (Short Wave)

FC Arbitrated Loop Mode Installation

This section provides the steps for installing and configuring RAID systems and Sun servers for Secure Path operation in FC Arbitrated Loop mode.

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 the RAID system and install the PCMCIA cards in the controllers.

   NOTE: Secure Path V2.1 for Sun Solaris requires StorageWorks ACS version 8.5F software on the RAID storage system.

2. Power ON the 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. Additionally, the LUN(s) must be visible from the Solaris Server using the *format* command.

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 RAID storage system controllers are in Transparent Failover Mode (see line 6 of example controller output) then they must be reconfigured for Multiple-bus Failover Mode. This is accomplished using the commands below.

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.

When the OTHER_CONTROLLER is available, enter:

HSG80 > **set multibus_failover copy = this_controller**

The controllers will restart in Multiple-bus Failover Mode. After the other controller has restarted, verify that both controllers are configured for Multiple-bus Failover 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:

Configured for MULTIBUS_FAILOVER with ZG90811309

In Transparent Failover Mode, the ALPAs of the left-hand ports are the same. Therefore if the left-hand top port had an ALPA of 71, the bottom left-hand port would also have an ALPA of 71.

When converting to Multiple-bus Failover Mode, it is recommended that a left-side or right side pair of ports be cabled for the loop configuration. A configuration in this manner will have one loop utilizing the top (left or right port) controller and one loop configuration utilizing the bottom (left or right port) controller for the second loop configuration for Secure Path. For Secure Path configurations, the identical ALPAs will not cause a problem as they are on different loops. In a large installation, it is recommended that the ALPAs be set to unique values to make explicit the path from an adapter to a port.

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 controllers to the hubs, as shown in Figure 3-1.
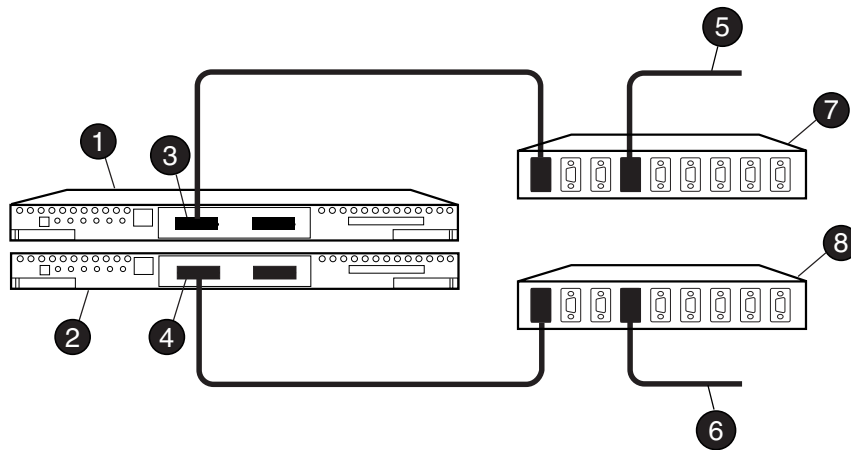
SHR-1604

Figure 3-1. Cabling Two RAID Controllers and Two FC Hubs

❶	Top HSG80 Controller	❺	FC cable to host bus adapter A
❷	Bottom HSG80 Controller	❻	FC cable to host bus adapter B
❸	Top Controller, port 1 (to host via top hub)	❼	FC-AL hub (top)
❹	Bottom Controller, 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 V2.1 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 LUN be configured on the RA8000/ESA12000 system, but a complete disk device configuration is recommended. Additionally, the LUN(s) must be visible from the Solaris Server using the *format* command.

8. Install or reinstall the RA8000/ESA12000 Solution Software V8.5 for Solaris 2.x 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. After installing the Solaris Solution software, invoke the config.sh in the opt/steam/bin (or the default installation directory selected), and perform the following two steps:

   a. Add the new adapter(s) to the host system and configure the new adapters for the intended targets on the RAID storage system. When adding the new FC adapter to the system, it is important to also add support for the *target* that is associated with the *ALPA* that is set for the host port. For example, if host port 1 is configured for ALPA 71, the target value assigned to this adapter will be 65. This change is made via the */opt/steam/config.sh* utility, under option 20. The target to ALPA conversion is included in Appendix D.

   NOTE: If you had selected the default installation path for the CPQhsg80 package, invoke**: /opt/steam/bin/config.sh** *Option 20*. If you chose an alternate location during the installation of the CPQhsg80 package, invoke: ***your area*/steam/bin/config.sh** *Option 20.*

   b. Reboot the server(s) and verify that the targets on the RAID storage system are visible on both adapters. This critical step ensures that Secure Path will be able to configure the server. If the two paths are not visible, refer to the *RA8000/ESA12000 Solution Software V8.5 for Sun Solaris – Installation and Reference Guide* to resolve the problem.

10. After the server has been rebooted, 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. Inspect the connection settings. Enter:

       HSG80 > **show connections**

       Example of the "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, as described in Chapter 4.

FC Fabric Mode Installation

This section provides the steps for installing and configuring RAID system(s) and Sun server(s) for Secure Path operation in FC Fabric (Switch) mode.

> **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 the RAID system and install the PCMCIA cards in the controllers.

   NOTE: Secure Path V2.1 for Sun Solaris requires StorageWorks ACS version 8.5F software on the RAID storage system.

2. Power ON the 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. Additionally, the LUN(s) must be visible from the Solaris Server using the *format* command.

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, with reference line numbers appended.

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 = 5000-1FE1-0000-8923'	12.
PORT_1_TOPOLOGY = FABRIC (fabric up)	13.
Address = 021000	17.
Host PORT_2:	14.
Reported PORT_ID = 5000-1FE1-0000-8924	15.
PORT_2_TOPOLOGY = FABRIC (connection down)	16.
NOREMOTE_COPY	18.
Cache:	19.
64 megabyte write cache, version 0012	20.
Cache is GOOD	21.
No unflushed data in cache	22.
CACHE_FLUSH_TIMER = DEFAULT (10 seconds)	23.
Mirrored Cache:	24.
64 megabyte write cache, version 0012	25.
Cache is GOOD	26.
No unflushed data in cache	27.
Battery:	28.
NOUPS	29.
FULLY CHARGED	30.
Expires: 16-DEC-2001	31.

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

    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.

    When the OTHER_CONTROLLER is available, enter:

    HSG80 > **set multibus_failover copy = this_controller**

    The controllers will restart in Multiple-bus Failover Mode. After the other controller has restarted, verify that both controllers are configured for Multiple-bus Failover 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:

    Configured for MULTIBUS_FAILOVER with ZG90811309

    In Transparent Failover Mode, under fabric configuration, both left hand ports share the same World Wide Port Name(WWPN). Similarly, both right hand ports share the same World Wide Port Name.

    When changing the HSG80 pair from Transparent Failover Mode to Multiple-bus Failover Mode in fabric, however, the World Wide Port Names (WWPN) for the different host ports are all unique. This information is necessary when using the */opt/steam/config.sh* utility to assign the WWPN to target mapping (Step 9) for configuring the new adapter(s).

    For example, in Transparent Failover Mode, host port 1 has a WWPN of 5000-1FE1-0000-8921. This is the same for the top and bottom controllers. When the controllers are configured for Multiple-bus Failover Mode, the WWPN for port 1 of the top controller will change to 5000-1FE1-0000-8923, while host port 1 of the lower controller will have a

WWPN of 5000-1FE1-0000-8921. The target to WWPN map must reflect these different values.

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 storage 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.

6. Cable the Fibre Channel adapter and the RAID storage system controllers to the SAN Switches, as shown in Figure 3-3.
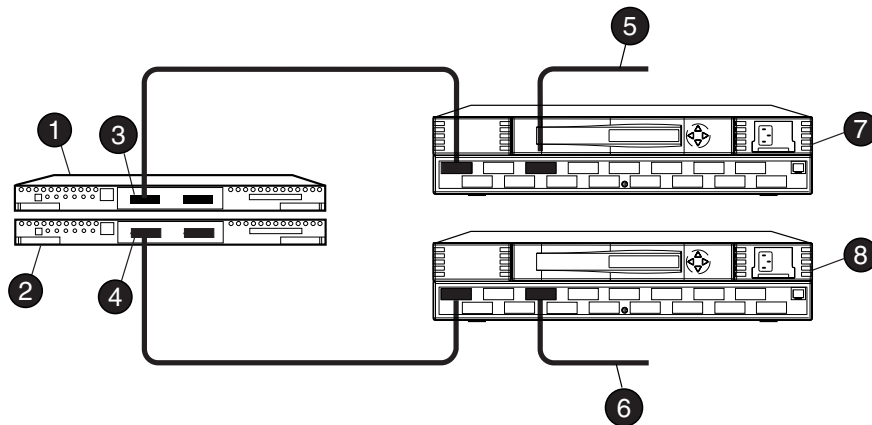
SHR-1653

Figure 3-2. Cabling Two RAID Controllers and Two SAN Switches

❶ Top HSG80 Controller A

❷ Bottom HSG80 Controller B

❸ Top Controller, port 1 (to host via top switch)

❹ Top Controller, port 1 (to host via bottom switch)

❺ FC cable to host bus adapter A

❻ FC cable to host bus adapter B

❼ SAN Switch (top)

❽ SAN Switch (bottom)

7. Power on the server.

8. Boot the system using the reconfiguration switch as follows:

For Solaris 2.6: ok> **boot –r**

NOTE: Secure Path V2.1 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 and is visible from the Solaris Server using the *# format* command.

9. Install or reinstall the RA8000/ESA12000 Solution Software V8.5 for Solaris 2.x and configure the Fibre Channel drivers for fabric mode. This is done with the /opt/steam/bin/config.sh utility using *Option 20*.

NOTE: If you had selected the default installation path for the CPQhsg80 package, invoke**: /opt/steam/bin/config.sh** *Option 20.* If you chose an alternate location during the installation of the CPQhsg80 package, invoke: ***your area*/steam/bin/config.sh** *Option 20.*

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 fabric instances of the World Wide Port Names (WWPNs).

Verify that the correct World Wide Port Names (WWPN) have been mapped to targets. This information is found in the output displayed using the following commands:

HSG80> **show this**

HSG80> **show other**

10. After the server has booted, check the RAID storage system 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 Name	Operating system	Controller	Port	Address	Status	Unit Offset
!NEWCON32	SUN	THIS	1	000001	OL this	0
HOST_ID=1000-00E0-6940-123C				ADAPTER_ID=2000-00E0-6940-123C		
!NEWCON34	SUN	OTHER	1	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**

The system is now ready for the installation of the Secure Path Software in Chapter 4

Chapter **4**

Installing Secure Path Software

This chapter provides the procedures to install a *new* Secure Path software configuration. For information on upgrading *existing* Secure Path configurations to Secure Path V2.1, and/or from a FC hub to SAN switch (FC fabric), reference Appendix B.

Prerequisites

Verify that the following requirements are met:

- The *StorageWorks Solution Software v8.5 for Sun Solaris* is installed on the Sun server.

- The *StorageWorks ACS V8.5F* firmware is installed on the RAID storage systems.

- The procedures in Chapter 3, *Hardware Setup* are successfully completed.

- Only one physical connection (path) exists between each RAID controller and each host bus adapter.

- At least one LUN is configured on the RAID storage system and is visible to the server from both paths. Ideally, the RAID storage systems are configured with all of the desired storagesets.

Installing Secure Path Software

Install Secure Path software as follows:

> ⚠ **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.

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 | grep vold

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

   If *vold* **i**s currently running:

   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_v21_sun/solaris

   d. Continue with step 3.

   If *vold* **is not** currently running:

   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_v21_sun/solaris

d. Continue with step 3.

3. Install Secure Path software, *CPQswsp*, on the Sun Solaris servers. The Secure Path software is installed using the Solaris "pkgadd" utility. Enter:

 # pkgadd –d pkgs

Below is a sample successful installation script.

IMPORTANT: As shown in the sample installation, the post-install script displays a warning that the driver (*mda*) failed to attach. This is an expected warning as the Secure Path has not been completely configured. (After the configuration files are generated and the server rebooted, the driver will successfully attach).

However, if a configuration error is encountered, refer to the *Responding to a Configuration Error* section of this chapter.

Sample successful installation script:

 # pkgadd -d

The following packages are available:

  1 CPQswsp   SANworks Secure Path
          (sparc) 21.G

Select package(s) you wish to process (or 'all' to process all packages). (default: all) [?,??,q]:

Processing package instance <CPQswsp> from </tmp>

SANworks Secure Path
(sparc) 21.G

Copyright Compaq Computer Corporation 2000, All rights reserved.

[complete Copyright text]

 Using </opt> as the package base directory.
Processing package information.
Processing system information.
  3 package pathnames are already properly installed.
Verifying package dependencies.
Verifying disk space requirements.
Checking for conflicts with packages already installed.
Checking for setuid/setgid programs.

This package contains scripts which will be executed with super-user
permission during the process of installing this package.
Do you want to continue with the installation of <CPQswsp> [y,n,?] y

Installing SANworks Secure Path as <CPQswsp>

```
## Installing part 1 of 1.
/etc/init.d/spinit
/kernel/drv/ldLite
/kernel/drv/ldLite.conf
/kernel/drv/ldLite.conf.proto
... [ files are moved to respective path areas ]
[ verifying class <none> ]
/etc/rcS.d/S65spinit <linked pathname>
## Executing postinstall script.
drvconfig: Driver (mda) failed to attach
Warning: Driver (mda) successfully added to system but failed to attach
Generating Secure Path Coinfiguration files...

Installation of <CPQswsp> was successful.

<END of sample installation>
```

4. Reboot the server upon successful installation of the software.

   NOTE: If a configuration error was encountered during installation, refer to *the Responding to a Configuration Error* section in this chapter.

5. Verify the Secure Path configuration by running the Secure Path Maintenance Tool, *spmt*.

   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
```

Responding to a Configuration Error

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

The *spconfig* tool is designed as a first-time, non-reentrant configuration tool for the files *mda.conf*, *ldLite.conf*, *fca-pci.conf*, *sd.conf* and *fcaw.conf* all located in /kernel/drv.

The s*pconfig* tool requires at least one LUN with two visible paths on the server. This LUN allows *spconfig* to communicate with the RAID storage system to gather information required for the configuration files named above.

Some configurations may present too many combinations for *spconfig* to determine the desired HBA and RAID storage system combinations. In such cases, *spconfig* will make an attempt to configure, but if unsuccessful, automatically issues a message that it is unable to configure the specific configuration for Secure Path.

Should this situation present itself, the *spconfig* utility must be run interactively, requiring user input to define the configuration. Interactive configuration is accomplished by invoking *spconfig* with a switch to indicate operator intervention (-o) as follows:

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

Sample *spconfig* session:

Provided below is a sample *spconfig* session (partial), with comments regarding the prompt input required.

root# **/opt/CPQswsp/bin/spconfig -o -p /kernel/drv**

When invoked, *spconfig* lists the devices connected to the RAID storage system

/devices/pci@b,2000/fibre-channel@2/sd@0,0:c,raw

/devices/sbus@6,0/fcaw@2,0/sd@40,0:c,raw

Spconfig identifies the device, HBA and RAID storage system and queries if this represents a Secure Path device/target. Answer yes or no in response to each query. With a yes response, *spconfig* will gather information about that RAID storage system.

```
-------------------------------------
Found the following target:
   Device:     /dev/rdsk/c3t65d0s2
   HBA:        /pci@b,2000/fibre-channel@2
   RAID Array:    this  -> ZG81701026
                  other -> ZG81700977
-------------------------------------
Is this a valid SecurePath Device/Target? [y or n]:y
Talking to Controllers on /dev/rdsk/c3t65d0s2.
Found 13 Luns.
```

As *spconfig* displays other devices, HBAs and RAID storage system entries, respond with a yes or no to indicate if this entry is part of the Secure Path configuration.

```
-------------------------------------
Found the following target:
   Device:      /dev/rdsk/c2t64d0s2
   HBA:         /sbus@6,0/fcaw@2,0
   RAID Array:  this  -> ZG92810311
                other -> ZG92810388
-------------------------------------
Is this a valid SecurePath Device/Target? [y or n]:y
Talking to Controllers on /dev/rdsk/c2t64d0s2.
Found 19 Luns.
```

When the Secure Path HBA's and RAID storage systems have been identified, spconfig displays the complete list of Target/LUNs found.

Found	LUN ID	/dev/rdsk
Getting:	6000-1FE1-0000-3250-0009-8170-1026-0076	/dev/rdsk/c3t65d0s2
Getting:	6000-1FE1-0000-3250-0009-8170-1026-007A	/dev/rdsk/c3t65d0s2
Getting:	6000-1FE1-0000-3250-0009-8170-1026-007E	/dev/rdsk/c3t65d0s2
.		
.		
.		
Getting:	6000-1FE1-0000-3250-0009-8170-0977-0010	/dev/rdsk/c4t64d0s2
Getting:	6000-1FE1-0000-3250-0009-8170-0977-0011	/dev/rdsk/c4t64d0s2

spconfig generates the configuration files, *mda.conf* and *ldLite.conf*. It modifies and/or adds entries to *sd.conf*. If the configuration is for fabric, *spconfig* writes entries to the driver configuration files.

```
Completed modifications to sd.conf...

Completed modifications to ldLite.conf...

Completed modifications to mda.conf...

root#
```

spconfig has completed the necessary file creation and modifications and the system is ready for a configuration reboot.

Return to Step 5.

Adding and Deleting Units to the RAID Storage System

The initial installation for Secure Path V2.1 will configure the existing RAID systems, making all LUNs available to the host server.

In a production environment, however, the configuration may have to be changed with the addition or deletion of a LUN at the RAID storage system. The following sections provide the steps to add or delete a unit, allowing the server to acquire the new Target/LUN combinations.

> ⚠️ **WARNING:** For each RAID system in a production environment, make sure that all users have logged off the Sun Solaris servers and that all I/O to the RAID systems has ceased. Follow normal procedures to backup the storage systems before proceeding.

Adding a Unit

To add a unit to a Secure Path installation, proceed as follows:

1. Add the unit to the RAID storage system 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 D18**

   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

   From the server point of view there are two modes to consider, FC Arbitrated Loop and FC Fabric.

For each mode, there are three (3) types of additions to consider, depending on whether the RAID storage system and/or adapter pair is new or existing. Use Table 4-1 to identify the configuration scenario into which a unit will be added. The procedures for each configuration are provided in the sections that follow.

The files that require additional data entries are documented in Chapter 6. Editing the files of the Secure Path system requires a clear understanding of those file entries.

NOTE: Refer to Appendix D for a complete list of Arbitrated Loop Physical Addresses (ALPAs).

Table 4-1
Adding a Unit - Configuration Scenarios

Configuration Mode	RAID System	Adapter Pair
A. Arbitrated Loop	Existing	Existing
B. Arbitrated Loop	New	Existing
C. Arbitrated Loop	New	New (second pair)
D. FC Fabric	Existing	Existing
E. FC Fabric	New	Existing
F. FC Fabric	New	New (second pair)

A. Arbitrated Loop Mode - Adding a New Unit onto an *Existing* RAID System Currently Configured on an *Existing* Pair of Adapters.

1. On the server, in the /kernel/drv directory, edit the three configuration files as described in steps a through c, below.

    a. *mda.conf* - Add two new path entries for the Target/LUN.

    Example: Assume that the target is 64 and the new unit added is D18.

    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 previously.

    Example: Assume that the last used targ*N*-devName in *ldLite.conf* had the value '20'.

Targ21-devName = "6000-1FE1-0000-0D40-0090-8090-0656-0123";

   c. ***sd.conf*** – Verify that an entry exists in *sd.conf* matching the "*N*" value in the targ*N*-devName entry of the *ldLite.conf* file. In the example, targ21-devName was added. An entry must exist for target 21.

   Example:

name="sd" parent="/pseudo/ldLite@0" target = 21, lun=0;

2. Reboot the server, by entering:

   # **touch /reconfigure**

   # **reboot**

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

   # **format**

Inspect the device list and verify that the new target c*X*t*Y*d*Z* has been acquired and is now visible.

B. Arbitrated Loop Mode - Adding a New Unit onto a *New* RAID System Currently Configured on an *Existing* Pair of Adapters.

1. When adding a new RAID storage system into an existing loop, define a unique set of ALPAs for the ports that will be used. All ALPAs on a loop must be unique.

   In the examples, the existing RAID storage system has an ALPA pair of 71, 72 (Hex); the new system being added has unique ALPAs of 73, 74 (Hex), that map to decimal 63, 62. The decimal mapping is used in *mda.conf* below. Only one of the ALPAs is required. Assume 73.

   When the units are added to the RAID storage system, record the LUN IDs.

2. On the server, in the /kernel/drv directory, edit the three configuration files as described in steps a through c, below.

      a) ***mda.conf*** - Add two new path entries for the Target/ LUN.

      Example: Assume the target is 73 (hex), (maps to decimal 63), and the unit added is D18.

   name="mda" parent= "/sbus@3,0/fcaw@0,0" target=63 lun=18;

   name="mda" parent= "/sbus@b,0/fcaw@0,0" target=63 lun=18;

b) *ldLite.conf* – Add the new LUN IDs, recorded previously.

Example: Assume that the last used targ*N*-devName was '24'.

targ25-devName = "6000-1FE1-0000-0D40-0780-2324-0609-00E0";

The LUN ID will differ from that of another RAID system, as it will contain the new controller identification.

c) **sd.conf** – Verify that an entry exists in *sd.conf* matching the "*N*" value in the targ*N*-devName entry of the *ldLite.conf* file. In the example, targ25-devName was added and an entry must exist for 25.

Example:

name="sd" parent="/pseudo/ldLite@0" target = 25, lun=0;

3. Reboot the server, by entering:

touch /reconfigure

reboot

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

 # **format**

Inspect the device list and verify that the new target c*X*t*Y*d*Z* has been acquired and is now visible.

C. Arbitrated Loop Mode - Adding a New Unit
onto a *New* RAID System Configured onto a *New*
(Second) Pair of Adapters in the Server.

1. With a second pair of adapters, the configuration will now have a second pair of arbitrated loops to configure. Since the RAID storage systems are on separate loops, the ALPAs chosen will not conflict with those from the existing configuration. However, on the same loop, the ALPAs must be unique.

2. Assume that the second loop will have the default ALPAs of 71,72 (hex), that maps to 64,65 decimal.

3. When the RAID storage system is configured, use the CLI to display each of the LUN IDs and record these for use in the next steps.

4. On the server, in the /kernel/drv directory, edit the three configuration files as described in steps a through c, below.

a) ***mda.conf*** - Add two new path entries for the Target/LUN.

Example: Assume that the target is 71 (Decimal 65) and the new units added are D1, D2, D12. However, since the server now has a second pair of adapters, the parent="hardware_path" will change to reflect the new hardware path. The hardware path may be found by invoking

 # ./opt/steam/bin/config.sh

Using Option 20, *Adding /Changing Adapters*, select *Add Adapters* and the software will invoke a scan of the system. Once displayed, record hardware paths for the two new adapters. Do not actually add these adapters to the server. The example entries below show new Sbus adapters.

Path 1. (Add 1 entry per Unit created.)

name="mda" parent= "/sbus@4,0/fcaw@0,0" target=65 lun=1;

name="mda" parent= "/sbus@4,0/fcaw@0,0" target=65 lun=2;

name="mda" parent= "/sbus@4,0/fcaw@0,0" target=65 lun=12;

Path 2.

name="mda" parent= "/sbus@f,0/fcaw@0,0" target=65 lun=1;

name="mda" parent= "/sbus@f,0/fcaw@0,0" target=65 lun=2;

name="mda" parent= "/sbus@f,0/fcaw@0,0" target=65 lun=12;

b) ***ldLite.conf*** – Add the new LUN IDs, recorded previously.

Example: Assume that the last used targ*N*-devName was '24'.

targ25-devName = "6000-1FE1-0000-0D40-0780-2324-0609-00E0";

targ26-devName = "6000-1FE1-0000-0D40-0780-2324-0609-00F4";

targ27-devName = "6000-1FE1-000-0D40-0780-2324-0609-00A0";

The LUN ID will differ from that of another RAID system, as it will contain the new controller identification.

c) ***sd.conf*** – Verify that an entry exists in *sd.conf* matching the "*N*" value in the targ*N*-devName entry of the *ldLite.conf* file. In the example, three entries were created, targ25-devName, targ26-devName, targ27dev-Name. Therefore an entry must be added for each.

Example:

name="sd" parent="/pseudo/ldLite@0" target = 25, lun=0;

name="sd" parent="/pseudo/ldLite@0" target = 26, lun=0;

name="sd" parent="/pseudo/ldLite@0" target = 27, lun=0;

5. Reboot the server, by entering:

    # **touch /reconfigure**

    # **reboot**

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

    # **format**

    Inspect the device list and verify that the new target c*X*t*Y*d*Z* has been acquired and is now visible.

D. FC Fabric Mode - Adding a New Unit onto an *Existing* RAID System Currently Configured on an *Existing* Single Pair of Adapters.

1. On the server, in the /kernel/drv directory, edit the three configuration files as described in steps a through c, below.

    a) *mda.conf* - Add two new path entries for the host Target/LUN.

        Example: Assuming that the target is 124 and the new unit added is D18.

        name="mda" parent= "/sbus@3,0/fcaw@0,0" target=124 lun=18;

        name="mda" parent= "/sbus@b,0/fcaw@0,0" target=124 lun=18;

    b) *ldLite.conf* – Add the new LUN ID, recorded previously.

        Example: Assume that the last used targ*N*-devName was '20'.

        targ21-devName = "6000-1FE1-0000-0D40-0090-8090-0656-0123";

    c) *sd.conf* – Verify that an entry exists in *sd.conf* matching the "*N*" value in the targ*N*-devName entry of the *ldLite.conf* file. In the example, targ21-devName was added and an entry must exist for 21.

        Example:

        name="sd" parent="/pseudo/ldLite@0" target = 21, lun=0;

2. Reboot the server, by entering:

   # **touch /reconfigure**

   # **reboot**

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

   # **format**

   Inspect the device list and verify that the new target c*X*t*Y*d*Z* has been acquired and is now visible.

E. FC Fabric Mode - Adding a New Unit onto *New* RAID System Currently Configured on an *Existing* Single Pair of Adapters.

1. To add another RAID system into the FC fabric requires cabling from the switch to the controllers of the RAID storage system as described in Chapter 3, creation of the UNITS and recording of the LUN IDs. Additionally, it is required that the World Wide Port Names (WWPN) for the controllers be known.

   Using the CLI, the WWPNs can quickly and easily be determined.

   HSG80> **show this**

   The information displayed contains a section labeled Host PORT_1 and Host PORT_2. Below these labels are entries of the Reported Port_ID, which is the World Wide Port Name (WWPN) in the format:

   nnnn-nnnn-nnnn-nnnn

   Record the correct WWPN mapping to the ports cabled. If the ports on the left side of the controller are used, record the Host Port 1 values. If the ports are on the right side of the controller, record the Host Port 2 values. The example below displays the top controller of a dual-redundant pair. The cabling is on the left port and the right port has been set off line.

In this example, the value to record for the top left port is "5000-1FE1-0000-8483". Upon displaying the other controller, the value to record for the bottom left port is "5000-1FE1-0000-8481".

Example: (from HSG80> ***show this***)

Host PORT_1:

    Reported PORT_ID = 5000-1FE1-0000-8483

    PORT_1_TOPOLOGY = FABRIC (fabric up)

    Address   = 011500

Host PORT_2:

    Reported PORT_ID = 5000-1FE1-0000-8484

    PORT_2_TOPOLOGY = offline

    NOREMOTE_COPY

(from HSG80> ***show other***)

Host PORT_1:

    Reported PORT_ID = 5000-1FE1-0000-8481

    PORT_1_TOPOLOGY = FABRIC (fabric up)

    Address   = 011500

Host PORT_2:

    Reported PORT_ID = 5000-1FE1-0000-8482

    PORT_2_TOPOLOGY = FABRIC (connection down)

    NOREMOTE_COPY

2. On the server, in the /kernel/drv directory, edit the four configuration files as described in steps a through d, below.

  a. ***fcaw.conf*** (for Sbus adapters) or ***fca-pci.conf*** (for PCI adapters)

    Inspect the listing of the entries that denote the WWPN for the existing RAID storage system. The entries are of the form,

    target*N*_wwpn="*nnnnnnnnnnnnnnnn*";

    Example:

    target125_wwpn="50001fe100000d43";

The target values, *N*, start at 125 and are counted down. The first RAID storage system required entries of 125 and 124. Therefore, the next entry starts at the next lower value, 123.

For the new RAID system, assume the WWPNs of:

5000-1FE1-0000-3241 and 5000-1FE1-000-3243.

Create an entry for each World Wide Port Name.

target123_wwpn="50001FE100003241";

target122_wwpn="50001FE100003243";

b. ***mda.conf*** - Add two new path entries for the Target/LUN..

Example: Using the example above, targets 123 and 122 and units D0, D4 and D5 added, the following would be added:

Path 1 - the first hardware path

name="mda" parent= "/sbus@3,0/fcaw@0,0" target=123 lun=0;

name="mda" parent= "/sbus@3,0/fcaw@0,0" target=123 lun=4;

name="mda" parent= "/sbus@3,0/fcaw@0,0" target=123 lun=5;

Path 2 - the second hardware path

name="mda" parent= "/sbus@f,0/fcaw@0,0" target=122 lun=0;

name="mda" parent= "/sbus@f,0/fcaw@0,0" target=122 lun=4;

name="mda" parent= "/sbus@f,0/fcaw@0,0" target=122 lun=5;

c. ***ldLite.conf*** – Add the new LUN IDs, recorded earlier.

Example: Assume that the last used targ*N*-devName was '13'.

targ14-devName = "6000-1FE1-0000-0D40-0090-8090-0656-0123";

targ15-devName = "6000-1FE1-0000-0D40-0090-8090-0656-012E";

targ16-devName = "6000-1FE1-0000-0D40-0090-8090-0656-0130";

The LUN ID will differ from that of another RAID system, as it will contain the new controller identification.

d. ***sd.conf*** – Verify that an entry exists in *sd.conf* matching the "*N*" value in the targ*N*-devName entry of the *ldLite.conf* file. In the example, targ14-devName, targ15-devName, targ16-devName were added and an entry must exist for each. By default, *sd.conf* has entries of 0-15. Only an entry for 16 needs to be added.

Example:

```
name="sd" parent="/pseudo/ldLite@0" target = 16, lun=0;
```

3. Reboot the server, by entering:

    # **touch /reconfigure**

    # **reboot**

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

     # **format**

    Inspect the device list and verify that the new target c*X*t*Y*d*Z* has been acquired and is now visible.

F. FC Fabric Mode - Adding a New Unit onto a *New* RAID System Configured onto a *New* (Second) Pair of Adapters in the Server.

1. To add another RAID system into the fabric requires cabling from the server to the switch and from the switch to the controllers of the RAID system (Chapter 3). UNITS are created and their LUN IDs are recorded. Finally, the World Wide Port Names for the controllers are recorded.

    Using the CLI, the WWPNs can quickly and easily be determined.

    HSG80> **show this**

    The information displayed contains a section labeled Host PORT_1 and Host PORT_2. Below these labels are entries of the Reported Port_ID, which is the World Wide Port Name (WWPN) in the format:

    nnnn-nnnn-nnnn-nnnn

    Record the correct WWPN mapping to the ports cabled. If the ports on the left side of the controller are used, record the Host Port 1 values. If the ports are on the right side of the controller, record the Host Port 2 values. The example below displays the top controller of a dual-redundant pair. The cabling is on the left port and the right port has been set off line. In this example, the value to record for the top left port is "5000-1FE1-0000-8483". Upon displaying the other controller, the value to record for the bottom left port is "5000-1FE1-0000-8481".

    Example: (from HSG80> **show this**)

    Host PORT_1:

         Reported PORT_ID = 5000-1FE1-0000-8483

         PORT_1_TOPOLOGY = FABRIC (fabric up)

```
        Address      = 011500
   Host PORT_2:
        Reported PORT_ID = 5000-1FE1-0000-8484
        PORT_2_TOPOLOGY  = offline
        NOREMOTE_COPY

(from HSG80> show other )
   Host PORT_1:
        Reported PORT_ID = 5000-1FE1-0000-8481
        PORT_1_TOPOLOGY  = FABRIC (fabric up)
        Address      = 011500
   Host PORT_2:
        Reported PORT_ID = 5000-1FE1-0000-8482
        PORT_2_TOPOLOGY  = FABRIC (connection down)
        NOREMOTE_COPY
```

2. On the server, in the /kernel/drv directory, edit the four configuration files as described in steps a through d, below.

    a) *fcaw.conf* for the Sbus adapter; *fca-pci.conf* for the PCI adapter.

        Inspect the listing of the entries that denote the WWPN for the existing RAID system(s). The entries are of the form:

        target*N*_wwpn="*nnnnnnnnnnnnnnnn*";

        Example:

        target125_wwpn="50001fe100000d43";

        The new RAID storage system requires new entries to be made to the configuration file for the fibre-channel driver. For the Sbus driver, *fcaw.conf*; for the PCI driver, *fca-pci.conf*.

        The target values, *N*, start at 125 and are counted down. The first RAID storage system required entries of 125 and 124. Therefore, the next entry starts at the next lower value, 123.

        For the new RAID storage system, assume the WWPNs are: 5000-1FE1-0000-8981 and 5000-1FE1-000-8983

Locate the section in the driver configuration file specific to the driver type (either *fcaw.conf* or *fca-pci.conf*) and add the entries for the new RAID storage system as shown in the example below.

target123_wwpn="50001FE100008981";

target122_wwpn="50001FE100008983";

b) *mda.conf* - Add two new path entries for the Target/LUN.

Example: Using the example above, targets 123 and 122 and units D0, D10, D11, D12 and D25 added, add the following:

Path 1

name="mda" parent= "/sbus@3,0/fcaw@0,0" target=123 lun=0;

name="mda" parent= "/sbus@3,0/fcaw@0,0" target=123 lun=10;

name="mda" parent= "/sbus@3,0/fcaw@0,0" target=123 lun=11;

name="mda" parent= "/sbus@3,0/fcaw@0,0" target=123 lun=12;

name="mda" parent= "/sbus@3,0/fcaw@0,0" target=123 lun=25;

Path 2

name="mda" parent= "/sbus@f,0/fcaw@0,0" target=122 lun=0;

name="mda" parent= "/sbus@f,0/fcaw@0,0" target=122 lun=10;

name="mda" parent= "/sbus@f,0/fcaw@0,0" target=122 lun=11;

name="mda" parent= "/sbus@f,0/fcaw@0,0" target=122 lun=12;

name="mda" parent= "/sbus@f,0/fcaw@0,0" target=122 lun=25;

c) *ldLite.conf* – Add the new LUN IDs, recorded previously.

Example: Assume that the last used targ*N*-devName was '13'.

The LUN IDs for D0, D10, D11, D12, and D25 are added.

targ14-devName = "6000-1FE1-0000-8980-0090-8090-0656-0123";

targ15-devName = "6000-1FE1-0000-8980-0090-8090-0656-012E";

targ16-devName = "6000-1FE1-0000-8980-0090-8090-0656-0130";

targ17-devName = "6000-1FE1-0000-8980-0090-8090-0656-0132";

targ18-devName = "6000-1FE1-0000-8980-0090-8090-0656-0140";

The LUN ID will differ from that of another RAID storage system, as it will contain the new controller identification.

d) ***sd.conf*** – Verify that an entry exists in *sd.conf* matching the "***N***" value in the targ***N***-devName entry of the *ldLite.conf* file. In the example, targets 14 through 18 were added, therefore an entry must exist in *sd.conf* for each.

By default, *sd.conf* contains entries for targets 0-6, and 8-15. Target entries above 15 must be added in *sd.conf*.

Example:

```
name="sd" parent="/pseudo/ldLite@0" target=16 lun=0;

name="sd" parent="/pseudo/ldLite@0" target=17 lun=0;

name="sd" parent="/pseudo/ldLite@0" target=18 lun=0;
```

3. Reboot the server, by entering:

   # touch /reconfigure

   # reboot

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

   # format

   Inspect the device list and verify that the new target c*X*t*Y*d*Z* has been acquired and is now visible.

Deleting a Unit

1. On the RAID storage 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. <u>Record the LUN ID</u>.

    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 files as described:

    a. *mda.conf* – delete the two path entries to the Target/LUN.

    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 previously.

    Example:

    Targ21-devName = "6000-1FE1-0000-0D40-0090-8090-0656-0123";

    c. *sd.conf* – If a matching target value entry for the unit was added to *sd.conf*, as shown by the example below, delete the entry. The entry will have the format "parent =". Do not remove any other entries.

    Example: name="sd" parent="/pseudo/ldLite@0" target=18 lun=0;

    d. For Fabric Only:

    If the deleted UNIT was the last UNIT and the RAID system is to be taken out of a FABRIC configuration, then either the *fcaw.conf* (Sbus) or *fca-pci.conf* (PCI) will contain entries that should be deleted.

Inspect the listing of the entries that denote the WWPN for the RAID storage system and delete them. For example, if the entries shown below identify the WWPNs for the RAID storage system, then they should be deleted.

target123_wwpn="50001FE100008981";

target122_wwpn="50001FE100008983";

4. Reboot the server by entering the following command:

    # **touch /reconfigure**

    # **reboot**

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

    # **format**

    Inspect the device list and verify that the deleted target, c*X*t*Y*d*Z* has been removed and is no longer visible.

Chapter **5**

Managing SANworks Secure Path

This chapter explains how to manage Secure Path using management tools.

Secure Path Management Tools

Secure Path provides two management tools:

- **spmt** - manages paths, displays stats, and permits CLI access to the controller.

- **spinit** – manages the spdaemon that detects path event and sends e-mail notification to a specified mail address.

spmt Commands

Table 5-1 lists the command options of the *spmt* utility. Command format and usage information follows.

<table>
<tr><td colspan="2">Table 5-1
spmt Command Options</td></tr>
<tr><td>Commands</td><td>Action</td></tr>
<tr><td>display</td><td>Displays status and information about Secure Path devices.</td></tr>
<tr><td>cli</td><td>Invokes a Command Line Interpreter (CLI) session to the RAID controller.</td></tr>
<tr><td>toggle</td><td>Switches the I/O to the standby path.</td></tr>
<tr><td>restart</td><td>Sends a CLI RESTART command to a specified controller.</td></tr>
<tr><td>shutdown</td><td>Sends a CLI SHUTDOWN command to a specified controller.</td></tr>
<tr><td>restore</td><td>Restores a Secure Path device to its user-defined (via CLI) PREFERRED_PATH.</td></tr>
<tr><td>remove</td><td>Quiesces paths for a specified host bus adapter (HBA).</td></tr>
<tr><td>reconfig</td><td>Activates paths for a specific HBA.</td></tr>
</table>

spmt Command Format and Usage

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. This number is contained as the *Y* value is the Secure Path device path: c*X*t*Y*d*Z*. (i.e., Device: c3t**2**d0).

Each field displayed in the output is described in Table 5-2. A sample follows.

Table 5-2 Fields Displayed by "spmt display"		
Field	**Value**	**Meaning**
Device (File)	c*X*t*Y*d*Z*	The Secure Path device
Status (of device)	operational	The Secure Path device can be accessed on at least one path.
	dead	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 of the storage RAID system.
State	online	Active path for the Secure Path device
	standby	Alternate path for the Secure Path device
	failed	Path is unavailable for I/O
	quiesced	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.

Example:

 # spmt display –t 9

(SBus target/LUN display)

```
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
```

(PCI target/LUN display)

```
Device: clt35d0    Status: Operational
Storage System: 5000-1fe1-0000-8920
LUN: 6000-1fe1-0000-8920-0009-9030-5234-00a9
============================================
Controller    Unit   State   HBA           Path
============================================
ZG90305234  D45    standby  pci1242,46430  /pci@b,2000/fibre-channel@2
ZG92810434  D110   online   pci1242,46431  /pci@f,2000/fibre-channel@2
```

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:

> *target_number* is the Secure Path target assigned to the storage unit, contained as the *Y* value is the Secure Path device path: c*X*t*Y*d*Z* (i.e., Device: c3t**2**d0).

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 multiple 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, contained as the *Y* value is the Secure Path device path: c*X*t*Y*d*Z* (i.e., Device: c3t**2**d0).

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 restore

The *spmt restore* command moves all online LUNs to their user-defined PREFERRED_PATH (this_controller or other_controller) specified in Chapter 3. This command takes no arguments and will operate on all LUNs. (See the related command, *spmt toggle*).

spmt remove

The *spmt remove* command quiesces the path for a specified host 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). 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.

To restore the user-defined PREFERRED_PATH, use the *spmt restore* command.

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 *spinit* 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 is a standard network internet address that 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 added or modified as part of the Secure Path V2.1 installation.

Table 6-1
Configuration Files Added / Modified by Secure Path V2.1

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

Modified Files	Description
/etc/driver_classes	Registers the IdLite driver
/etc/devlink.tab	Defines devlinks entry for the IdLite
/kernel/drv/fcaw.conf /kernel/drv/fca-pci.conf	Assigns a target number to a controller's World Wide Port Name (WWPN) - fabric mode.

Table 6-1
Configuration Files Added / Modified by Secure Path V2.1 *continued*

Added Files	Description
/kernel/drv/sd.conf	▪ Removes selected entries created by the *RAID Solution Software for Sun Solaris* (platform kit). ▪ Adds Secure Path entries for target values greater than 15.

File/Entry Format

/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, the following entry has been added to the *devlink.tab* file:

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

/kernel/drv/fcaw.conf
/kernel/drv/fca-pci.conf

In a fabric configuration, a target must be assigned to a World Wide Port Name (WWPN). Target values must be in the range of 125 down to 16, inclusive. For example, to assign target 125 to the port number 5000-1FE1-0000-0D43, *fcaw.conf* would have the following entry:

target125_wwpn="50001FE100000D43";

/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 target assigned to the controller port, and the LUN assignment.

In a loop configuration, the target assigned is related to the Arbitrated Loop Physical Address (ALPA). Appendix D provides a list of valid ALPAs.

Example entry for the Sbus adapter:

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;

In a fabric configuration, the target assigned to the controller port is the target number assigned to the port number in the *fcaw.conf* or *fca-pci.conf* file.

Example entry for the PCI adapter:

name="mda" parent="/pci@b,2000/fibre-channel@2" target=125 lun=0 qdepth=32;

name="mda" parent="/pci@f,2000/fibre-channel@2" target=124 lun=0 qdepth=32;

/kernel/drv/ldLite.conf

Secure Path device files are configured by the ldLite driver utilizing the *ldLite.conf* file. Subsequently, the first entry assigns a driver (ldLite) with a pseudo hardware path for a SCSI class.

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

The entries designate the specific units identified by the World Wide LUN ID assigned by the RAID storage system. For every pair of LUN assignments in *mda.conf* there is matching targ*N*-devName in *ldLite.conf*. The target number, *N*, assigns a Secure Path device number to a unit on a RAID storage system. The *ldLite.conf* target number, *N*, must be unique. The value assigned must have a corresponding entry in the /kernel/drv/sd.conf file. Examples of entries in *ldLite.conf* are as follows:

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

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

/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). The target numbers assigned must match the targ*N* numbers assigned in *ldLite.conf*. For example, Secure Path device target 20 would have the following entry:

name="sd" parent="/pseudo/ldLite@0" target=20 LUN=0;

Command Console LUN

The Command Console LUN (CCL) is a special pseudo disk device on the RAID storage system that allows it to communicate. Entries for the CCL in the *mda.conf*, *ldLite.conf* and *sd.conf* are similar to other LUNS with the following differences:

- *mda.conf*

    If the CCL is enabled, the LUN assigned to the CCL can be determined by issuing the following CLI command:

    HSG80> show this_controller

    The LUN ID assigned to the CCL is displayed in the controller data. Similar to any storage LUN on the RAID storage system, there must be two entries for the CCL in *mda.conf* – one for each path.

- *ldLite.conf*

    The World Wide LUN ID that is needed in *ldLite.conf* is created by appending the Node ID of the RAID storage system with the SCSI ID of the CCL device (HSG80CCL).

    The Node ID can be determined by issuing the CLI command:

    HSG80> **show this_controller**

    The Node ID is a 16-character hexidecimal value displayed as the NODE_ID in the Controller data.

    The SCSI device ID of the CCL must also be converted to a hexidecimal value. Thus HSG80CCL converts to 4853-4738-3043-434C.

For example, to assign the CCL to target 20 of a SANworks Storage System with a Node ID of 5000-1FE1-0001-ED10, *ldLite.conf* must have the following entry:

```
targ20-devName = "5000-1FE1-0001-ED10-4853-4738-3043-434C"
```

Appendix A

Glossary

ALPA   *Arbitrated Loop Physical Address.* A value used to identify a
             port in a Fibre Channel Arbitrated Loop topology.

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 serial number.

Fabric   A network comprised of high-speed fibre connections resulting
             from the interconnection of switches and devices. A fabric is an
             active and intelligent non-shared interconnect scheme for nodes.

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.

Hub   A Fibre Channel device that connects nodes into a logical loop
             by using a physical star topology. Hubs will automatically
             recognize an active node and insert the node into the loop. A
             node that fails or is powered off is automatically removed from
             the loop.

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 states:

- **operational -** the Secure Path device can be accessed on at least one path.

- **dead -** all paths used by this Secure Path device have failed.

Switch	A Fibre Channel, multiple port device that provides virtual I/O paths between Fibre Channel devices such as servers, storage systems and other Storage Area Network (SAN) switches. A switch is an intelligent, programmable connection component of a Storage Area Network.
Target	A target is the addressable device to logical I/O units (LUNs). The target value assigned to the paths to the storage device in the *mda.conf* file depend on the Fibre Channel topology.

For FC Arbitrated Loop, the target is based on the ALPA assigned to the port on the controller for that path. The ALPA number on the RAID controller translates to a target number on the host. The translation table is found in Appendix D of this guide.

For FC switched fabric, a target is assigned to a WWPN. This target can have values between 16 and 125.

Topology	An interconnection scheme that allows multiple Fibre Channel ports to communicate. Arbitrated Loop and switched fabric are examples of Fibre Channel topologies.

Appendix **B**

Secure Path Configuration Upgrades

The Secure Path upgrade scenarios discussed in this appendix are as follows:

Section	Existing Configuration	Intended Configuration
A	V2.0, Hub/Arbitrated Loop	V2.1, Hub/Arbitrated Loop
B	V2.0, Hub/Arbitrated Loop	V2.1, Switch/Fabric
C	V2.1, Hub/Arbitrated Loop	V2.1, Switch/Fabric
C (Alt)*	V2.1, Hub/Arbitrated Loop	V2.1, Switch/Fabric

* This alternate method for Secure Path V2.1 loop to switch conversion method involves applying edits to system and kernel level files. It is not intended for general use, and should be only be performed by the most knowledgeable system support experts.

⚠ **CAUTION:** The installation instructions that follow require that no I/O is in progress to the target/LUNs on the RAID systems communicating with the Sun server that is to be upgraded. Also, follow normal procedures to perform a complete backup before making any changes to the Secure Path configuration.

A. Upgrading a V2.0 Hub/Arbitrated Loop to a V2.1 Hub/Arbitrated Loop

This section explains how to upgrade Secure Path V2.0 to Secure Path V2.1 in an existing hub-based FC Arbitrated Loop configuration.

When Secure Path is upgraded from V2.0 to V2.1, it preserves the existing configuration files, *mda.conf*, *ldLite.conf* and any entries added to the *sd.conf* files by the Secure Path V2.0 application. This includes the existing targets as seen by the *format* command.

After the software upgrade, new UNITS may be added on the RAID (reference *Adding Units* in Chapter 4).

When Secure Path V2.1 is installed as an upgrade, it will:

- Overlay new versions of the Secure Path drivers

- Update the utilities in the /opt/CPQswsp/bin area

- Invoke a script that, for entries added to V2.0, modifies the existing parameter: class = "scsi" to parent = "pseudo/ldLite@0". This prevents "sd", the class driver, from unnecessary SCSI probes of devices during the booting process.

The V2.1 upgrade installation is automatic once invoked using the standard Sun Solaris application installation procedures, as described in Chapter 4, *Installing Secure Path Software*.

B. Upgrading a V2.0 Hub/Arbitrated Loop to a V2.1 Switch/Fabric

To upgrade Secure Path V2.0 in an existing FC Arbitrated Loop, to Secure Path V2.1 in a switch-based FC Fabric configuration requires that:

- Existing configuration mapping of target/LUNs is maintained before and after the change of configuration modes to preserve existing targets as seen by the *format* command.

- The Secure Path configuration files are modified to accommodate the transition from the ALPAs of the loop environment to the World Wide Port Names of the Switch/Fabric environment.

- Existing UNITS on the RAID remain constant during the configuration conversion. (New UNITS may be added after the conversion, as documented in the *Adding Units* section of Chapter 4).

To upgrade the software and convert the configuration, performing the following steps:

1. Copy */kernel/drv/ldLite.conf* to */kernel/drv/ldLite.conf.ref* To simplify a later step, print a copy for reference.

2. Remove Secure Path V2.0, using the following Solaris command:

   # **pkgrm CPQswsp**

3. Convert the RAID storage system from loop mode to fabric mode and record the World Wide Port Names assigned to each port used in the Secure Path configuration. Move the corresponding cables from the fibre channel hubs to fibre channel switches.

4. Perform the next actions to change the mode of the driver(s) and create entries in */kernel/drv/sd.conf* to the target/LUNs on the RAID array:

   a. At the server, invoke the Solaris configuration utility kit. Enter:

      # **/opt/steam/bin/config.sh**

   b. Select Option 20, *Add/Change Adapters*.

   c. Select Option 4, *Modify an Adapter* and select each adapter to be used in the Secure Path configuration.

   d. Update the mode from loop to fabric, and when the WWPN is requested, input the values as recorded in step 3. Associate the correct adapter to the specific controller port on the RAID system.

5. Reboot the server with a reconfiguration. The following is recommended:
   # **touch /reconfigure**
   # **reboot**

   Secure Path requires that at least one target/LUN is visible from the server. After you reboot the server, verify that at least one target/LUN is visible from the server to the RAID array, from each adapter. This condition must be met before proceeding to the next step.

6. Install Secure Path V2.1.
   Secure Path V2.1 installation generates new configuration files in */kernel/drv*. Specifically, *mda.conf* and *ldLite.conf*. It also adds entries to the *fcaw.conf* or *fca-pci.conf* files of the WWPN bindings for the fibre channel driver(s). If necessary, the file, /kernel/drv/sd.conf will be updated.

7. Compare the two versions of the *ldLite.conf* files. Both lists of entries should be have the same targ*T*-devName paired with the same LUN ID string.

Example:

targ12-devName="6000-1FE1-0000-3250-0009-8170-0977-0010";

In this example, the value of *T* is 12 and is paired to a specific LUN ID at the Raid storage system. At the same time, *T* is the Target value used in /kernel/drv/sd.conf and represents the '*Y*' value in c*X*t*Y*d*Z* device files.

Verify that all targ*T*-devNames and World Wide LUN ID are paired identically in the new and old versions of the *ldLite.conf* file. Adjust the mapping accordingly.

C. Upgrading a V2.1 Hub/Arbitrated Loop to a V2.1 Switch/Fabric

This section explains how to change a Secure Path V2.1, hub-based FC Arbitrated Loop configuration to a Secure Path V2.1, switch-based FC Fabric configuration.

1. Copy /kernel/drv/ldLite.conf to /kernel/drv/ldLite.conf.ref. To simplify a later step, print a copy for reference.

2. Remove Secure Path V2.1 using the standard Solaris command:

   # pkgrm CPQswsp

3. Convert the RAID storage system from its loop mode to fabric mode and record the World Wide Port Names assigned to each port used in the Secure Path configuration. Move the corresponding cables from the fibre channel hubs to fibre channel switches.

4. Perform the next actions to change the mode of the driver(s) and create entries in */kernel/drv/sd.conf* to the target/LUNs on the RAID system:

   a. At the server, invoke the Solaris configuration utility. Enter:

      # /opt/steam/bin/config.sh

   b. **S**elect Option 20, *Add/Change Adapters*.

   c. Select Option 4, *Modify an Adapter* and select each adapter to be used in the Secure Path configuration.

   d. Update the mode from loop to fabric, and when the WWPN is requested, input the values as recorded in step 3. Associate the correct adapter to the specific controller port on the RAID storage system.

5. Reboot the server with a reconfiguration. The following is recommended:

 # touch /reconfigure

 # reboot

Secure Path requires that at least one target/LUN be visible from the server. When you reboot the server, verify that <u>at least one target/LUN is visible from the server to the RAID storage system, from each adapter.</u> Only if this condition is met should you proceed to the next step.

6. Reinstall Secure Path V2.1 using the standard Solaris *pkgadd* utility. The installation of Secure Path V2.1 will generate new configuration files in /kernel/drv - specifically, *mda.conf* and *ldLite.conf*. Additionally, the installation will add entries to the *fcaw.conf* or *fca-pci.conf* files for the WWPN bindings for the fibre channel driver(s). If necessary, /kernel/drv/sd.conf will be updated.

7. Compare the two versions of the *ldLite.conf* files. Both lists of entries must have the same targ$T$-devName paired with the same LUN ID string. For example:

   targ12-devName="6000-1FE1-0000-3250-0009-8170-0977-0010";

   In this example, the value of T is 12 and is paired to a specific LUN ID at the RAID storage system. At the same time, the value T is the Target value used in /kernel/drv/sd.conf and represents the 'Y' value in cXtYdZ for the device files.

   Verify that all targT-devNames and World Wide LUN ID are paired identically in the new and old versions of *the ldLite.conf* file. Adjust the mapping accordingly.

C. (Alt.) Upgrading a V2.1 Hub/Arbitrated Loop to a V2.1 Switch/Fabric

This section provides an alternate method to change a Secure Path V2.1, hub-based FC Arbitrated Loop configuration to a Secure Path V2.1, switch-based FC Fabric configuration. This conversion is accomplished by applying edits to system and kernel level files. This conversion is not intended for general use. It should be performed only by the most knowledgeable system support experts.

1. Convert the RAID storage system from its FC Arbitrated Loop mode to Fabric mode and record the World Wide Port Names assigned to each port used in the Secure Path configuration. Move the corresponding cables from the fibre channel hubs to SAN switches.

2. Perform the next actions to change the mode of the driver(s) and create entries in /kernel/drv/sd.conf to the target/LUNs on the RAID storage system:

   a. At the server, invoke the Solaris configuration utility. Enter:

      # **/opt/steam/bin/config.sh**

   b. Select Option 20, *Add/Change Adapters.*

   c. Select Option 4, *Modify an Adapter* and select each adapter to be used in the Secure Path configuration.

   d. Update the mode (from loop to fabric) and when the WWPN is requested, input the values as recorded in step 3. Associate the correct adapter to the specific controller port on the RAID storage system.

3. At the server, examine /kernel/drv/mda.conf and record the Target mappings to the specific RAID storage systems. In the simplest case, one RAID storage system will have two Target assignments. For multiple RAID systems, there may be multiple Target assignments that are specific to one or more RAID systems.

   Example: (1 RAID system)
   Targets 64, 65 for RAID_1

   Example: (2 RAID systems)
   Targets 64, 65, for RAID_1 and Targets 62,63 for RAID_2

4. The supported Secure Path adapters for fibre channel are the JNI 64-bit Sbus adapter and the JNI 32-bit PCI adapter. The drivers have configuration files in /kernel/drv**,** as *fcaw.conf* or *fca-pci.conf.*

   Secure Path only supports pairs of adapters of the same type. Determine the adapter type used in the Secure Path configuration.

5. With an editor, open the respective configuration file and create entries as described below and shown in the examples.

   For each target found in the *mda.conf* file from Step 3, add an entry for the WWPN. This entry provides a binding for the driver to the respective World Wide Ports of the controller on system boot. The bindings prevent the driver from attaching to other WWPNs in the fabric.

   Example: (1 RAID system)

   Targets 64, 65 with WWPNs of 5000-1FE1-0000-0971 and WWPN of 5000-1FE1-0000-0973.

NOTE: When WWPNs are entered into the fcaw.conf and/or fca-pci.conf files, the hyphens are removed.

The entries have the form: target*T*_wwpn="nnnnnnnnnnnnnnnn";
This example shows two entries created as follows:

target64_wwpn="50001FE100000971";

target65_wwpn="50001FE100000973";

Example: (2 RAID systems)

Targets 64, 65, 63, 62 with WWPNs of:

Targets 64, 65: 5000-1FE1-0000-4322, 5000-1FE1-0000-4324

Targets 62, 63: 5000-1FE1-0001-8891, 5000-1FE1-0001-8893

The four entries are:

target64_wwpn="50001FE100004322";

target65_wwpn="50001FE100004324";

target62_wwpn="50001FE100018893";

target63_wwpn="50001FE100018891";

The entries may be placed at the top of the file or included in the section identified by the label "Configuration flag - def_wwXn_binding". However, the StorageWorks Solution Software for Sun Solaris has already added parameters for per-instance bindings, marked by a CPQhsg80 header. It is recommended that the target*T*_wwpn bindings be inserted after the CPQhsg80 trailer comment.

6. Reboot with a reconfiguration switch. The recommended procedure is:

touch /reconfigure
reboot

Use the *format* command to verify that the targets have been acquired.

Appendix **C**

Removing SANworks Secure Path Software

This appendix describes how to remove SANworks 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 SANworks 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. After 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 storage system.

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. The recommended procedure is:

 # touch/reconfigure

 # reboot

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 D*n***

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 D*n 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 **D**

Valid ALPA Settings

About ALPA Settings

Table D-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 D-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	19	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

Table D-1
ALPA Settings *continued*

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)
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.

Index