COMPAQ

StorageWorks Secure Path V3.0 for Windows NT

Installation and Reference Guide

AA-RL4SB-TE

Second Edition (January, 2000)
Compaq Computer Corporation

Notice

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

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

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

StorageWorks Secure Path V3.0 for Windows NT
Second Edition (January, 2000)
AA-RL4SB-TE

Contents

About This Guide

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

Text Conventions

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

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

Symbols in Text

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

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

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

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

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

Symbols on Equipment

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

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

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

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

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

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

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

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

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

Rack Stability

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

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

Getting Help

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

Compaq Technical Support

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

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

Outside North America, call the nearest Compaq Technical Support Phone Center. Telephone numbers for world wide Technical Support Centers are

listed on the Compaq website. Access the Compaq website by logging on to the Internet at http://www.compaq.com

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

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

Compaq Website

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

Compaq Authorized Reseller

For the name of your nearest Compaq Authorized Reseller:

- In the United States, call 1-800-345-1518.
- In Canada, call 1-800-263-5868.
- Elsewhere, see the Compaq website for locations and telephone numbers.

Chapter 1

Theory of Operation

Overview of Secure Path for Windows NT

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

Secure Path version 3.0 allows a StorageWorks dual-controller RAID subsystem to be cabled on two or more independent SCSI, Fibre Channel Arbitrated Loop, or Fibre Channel Switch paths using two or more separate host bus adapters in each server. Version 3.0 provides support for single host server, Microsoft Cluster Server (MSCS) and Oracle Parallel Server (OPS) High Availability environments.

Secure Path monitors each path and automatically re-routes I/O to the functioning alternate path(s) should an adapter, cable, hub, 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.

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

Through the use of dual RAID controllers configured in multiple-bus mode operation and load distribution capability, Secure Path can also exploit the potential for improved data throughput and bandwidth performance.

Secure Path Technology

Key to Secure Path's functionality is the capability of dual StorageWorks RAID controllers to operate in an active/active implementation, referred to as dual-redundant multiple-bus mode. Multiple-bus mode allows each controller to process I/O independently of the other controller under normal operation. Available storage units are preferred to one or the other of the two controllers by setting a PREFERRED_PATH unit attribute. This attribute determines which controller is used for access at system boot time. During runtime, storage units may be moved between paths at any time through use of the Secure Path Management utility. On HSG80 RAID devices, storage units may also be accessed on each controller through either of two available ports.

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

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

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

Auto-Failback and Path Verification

Path verification and auto-failback are two features that augment Secure Path's automated path management capabilities. With auto-failback enabled, Secure Path will monitor failed paths and automatically return failed-over storage units to their original path(s), once the path has been restored. Anti-thrash filters are implemented to prevent ping-pong effects resulting from marginal or

intermittent conditions. The user may select auto or manual failback policy through use of the Secure Path Management utility.

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

Load Distribution

Secure Path version 3.0 takes advantage of the potential of multiple path access and enhances I/O performance through use of load distribution capability. With this feature enabled, Secure Path evenly distributes I/O operations across all available paths to a given storage unit.

Implementation

Secure Path's primary failover capability is implemented in a Windows NT filter driver called RaiDisk. RaiDisk implements support for the StorageWorks RAID Array multiple-bus mode of operation, multiple path access and provides all functions required for monitoring I/O and detecting path failures.

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

Path management is implemented using Secure Path Manager. Secure Path Manager is a client/server application that continuously monitors the multiple path storage environment and automatically updates the displayed configuration information based on current status. Secure Path Manager indicates which path is currently servicing each configured storage unit and displays the mode and state information for all available paths.

Secure Path Manager communicates with the RaiDisk driver through the Secure Path Agent. The Secure Path Agent is implemented as a Windows NT Service application that is installed on the host server along with the RaiDisk driver. The Secure Path Agent communicates with the Secure Path Manager through use of the TCP/IP protocol and the WinSock application programming interface. To minimize local area network traffic, display information is relayed from the Secure Path Agent to the Secure Path Manager only when changes in the configuration are detected by the RaiDisk driver. The Secure Path Agent will also notify StorageWorks Command Console (SWCC) clients when path failover or auto-failback operations are performed by RaiDisk.

Each software component of Secure Path makes use of the Windows NT event log facility to post error and informational messages as required.

The Secure Path Software Components

The Secure Path (v3.0) Software Kit for Microsoft Windows NT is comprised of the following software components:

- **HszDisk.sys** is a Windows NT class driver that works with StorageWorks RAID Array controllers to enhance on-line storage availability and fault-tolerance. HszDisk works in single-host and cluster environments to maintain optimum subsystem performance during controller and storageset error recovery operations.
- **RaiDisk.sys** is a Windows NT filter driver that provides support for multiple path access and multiple-bus mode operation with StorageWorks RAID Arrays. RaiDisk performs automatic failover of storagesets to the alternate path in the event of a primary path failure.
- **Secure Path Manager** is the client application used to manage multiple path StorageWorks RAID Array configurations. Secure Path Manager displays a graphical representation of the current multiple path environment and indicates the location and state of all configured storage units on each of the paths. To facilitate static load balancing, Secure Path Manager provides the capability to move storagesets between paths. Secure Path Manager can be run locally at the managed servers, or remotely at a management workstation.
- **Secure Path Agent** is the Windows NT service that communicates with the RaiDisk filter driver on the server and with the Secure Path Manager on the client side via the TCP WinSock interface. The Secure Path Agent makes use of the Windows NT application event log and will post error and informational messages as required.
- **Secure Path Setup** supports driver installation and de-installation with Windows NT 4.0

Chapter 2

Technical Description

Overview

This chapter provides general discussion of technical details of Secure Path configurations and features and storage path identification in a high availability environment.

Technical Description

Profiles

StorageWorks Secure Path Version 3.0 for Windows NT provides the capability of managing large configurations through a single instance of the Secure Path Manager. There are, however, certain practical limits on the configuration size that can be displayed and managed in a single window. Secure Path Manager uses the concept of the “managed entity” or “profile” to express this working configuration limit.

In essence, the managed entity or profile limits for Secure Path Manager are a maximum of 8 servers (host systems) connected to and sharing up to 8 storage systems configured for and connected in multiple-bus failover mode. The host systems may all be standalone servers or may be grouped into clusters as long as all servers in the profile have access to all of the storage systems listed in that profile. Please note that Secure Path itself does not provide any mechanism for synchronizing access to or guaranteeing the data integrity of storagesets shared across multiple standalone hosts or across several clusters.

Access to storagesets must be restricted to a single standalone server or a single "clustered" host set using the controller "access ID" unit attribute. Please reference your Solution Software Kit documentation for details.

The Secure Path Manager supports the creation of multiple profiles stored as separate files in the same directory in which it resides. Any given server, cluster or storage system may exist in multiple profiles as long as the profile configuration rules described above are followed.

Controller Ownership

Storage Systems that are multiple-bus capable generally contain a pair of redundant controllers and support one of two basic operational models: active/passive or active/active. In the active/passive model, all storagesets are assigned to one of the controller pair for I/O processing with the other controller inactive, but available as a substitute in the event of failure on the original. In the active/active model, I/O may be routed through both controllers simultaneously, providing better performance in addition to high availability.

The RA7000/8000 and ESA10000/12000, supported by Secure Path, implement a modified version of the active/active model. While I/O can be processed simultaneously by both controllers, any given storageset is "owned" or online to a host through only one controller. Ownership of a storageset may be transferred to the other controller at any time through a host initiated command sequence. However, since the ownership transfer results in controller cache flushing and I/O wind down, the storageset may become inaccessible for a period of several seconds to complete this sequence; purely arbitrary ownership transfers should be avoided by the user, and are never automatically initiated by Secure Path. Note that Secure Path automatically retries I/O requests that terminated in error due to ownership transfers and also queues new I/O requests until the ownership transfer has completed to insure data integrity.

Path Definition

Within Secure Path, a path is defined as the collection of physical interconnect components including Host Bus Adapters, switches or hubs, Fibre Channel cables, RAID array controllers and the ports on the controllers. Since the Secure Path driver component, RaiDisk, is positioned between the Port and Class driver layers of Windows NT, it can distinguish among physical paths only when elements of the SCSI equivalent address are different. (The following sections expand upon SCSI address elements definition for Fibre Channel configurations.) Some configurations may include multiple cascaded switches within a fabric with the switches connected

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

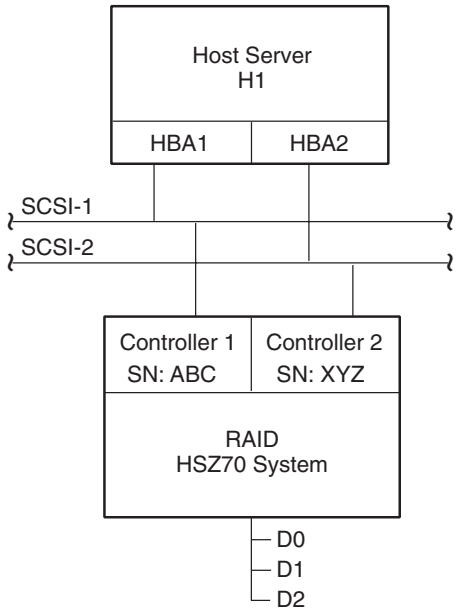
Path Definition for Parallel SCSI-based Configurations

In parallel SCSI, a path consists of the complete physical interconnection from a given host to a specific storageset in a RAID storage system. In Windows NT there are four bits of information that comprise the "address" of a given path to a specific storageset; they are, port number, bus number, target ID and logical unit number (LUN).

Port number is created by Windows NT and refers to a specific SCSI adapter; numbers are zero-based and are assigned in the order of discovery, hence they are relative and may change as a result of system reconfigurations (*i.e.*, adding or removing other SCSI adapters). (Secure Path Manager displays the port number in the column headed "HBA" (Host Bus Adapter) as shown in Figure 2-1.) Bus number is a value resulting from the design of the SCSI adapter itself and refers to the number of physically independent interconnects supported; this number is currently always zero for SCSI adapters running with Secure Path. The target ID and LUN are values which are set in the RAID Array controller in the unit name which is of the form "Dxxyy" in which 'xx' is the target number (0 – 15) and 'yy' is the LUN (0 – 7 for Windows NT). Note that if the target number is 0, it is dropped from the unit number designation, so the unit number D0 is understood to be LUN 0 on target 0 while D100 is LUN 0 on target 1. Every storageset configured on an RA7000 or ESA10000 must have a unique unit name assigned to it.

SCSI paths under Secure Path are relatively easy to understand because there are generally no more than two paths from a host to a specific LUN, the path addressing under Windows NT is adapted directly from SCSI-defined addresses and each path implies connection to a discreet controller. Since the RA7000 and ESA10000, by design, present an identical address space from both controllers, the only bit of address information which will be different

across the paths from a given host to a specific storageset is the port (HBA) number, as shown in Figure 2-1.



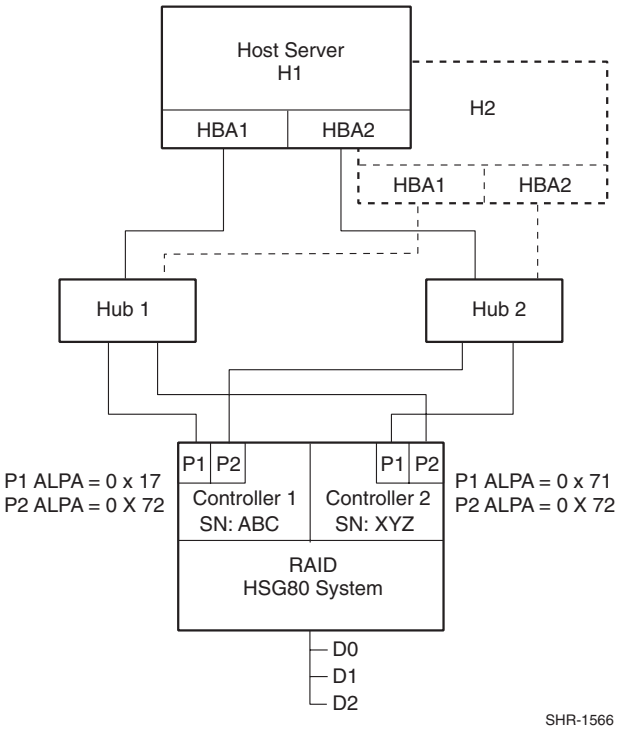
	Host	Controller Serial No.	Host Bus Adapter	Bus-Target-Lun
Drive D: D1	H1	ABC	1	0 –0 –1
	H1	XYZ	2	0 –0 –1

Figure 2-1. Path Definition in a SCSI based Secure Path Configuration

Path Definition for Fibre Channel Arbitrated Loop

In a Fibre Channel arbitrated loop (FC-AL) configuration, devices are accessed within Windows NT using conventional SCSI addressing terminology. As shown in Figure 2-2, Fibre Channel adapters are referred to as HBAs and are named and numbered by Windows NT as SCSI ports. The rest of the SCSI address (except the LUN) is actually created within the Fibre Channel's miniport driver and is derived from the ALPA (Arbitrated Loop Physical Address) assigned to each port on the RA8000/ESA12000 controllers. The LUN number is derived from the unit number assigned to the storageset within the controller using SWCC or CLI commands. Each connected node on an arbitrated loop must have a unique ALPA assigned. In

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



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

Figure 2-2. Path Definition in a Secure Path FC-AL Configuration

Note also that the LP6NDS35 miniport driver for the KGPSA Fibre Channel adapter uses a fixed mapping scheme to translate ALPA assignments to SCSI bus and target ID values. Appendix C provides a complete listing of KGPSA ALPA to SCSI mapping. Please also note that when installed in your system,

the adapter is instructed to perform scan-down, starting from the highest ALPA and moving downward. As shown in the first line of the path table in Figure 2-2, (and also in Appendix C), the adapter maps ALPA 0x71 to Bus 3, Target ID 3. (Even though the KGPSA has only a single physical Fibre Channel interconnect, it artificially expands the enumeration of buses to allow mapping the supported Fibre Channel ALPA address space into the Windows NT SCSI address space. Bus 0 is never used and we recommend that ALPAs below 0x71 be reserved for adapter assignments.)

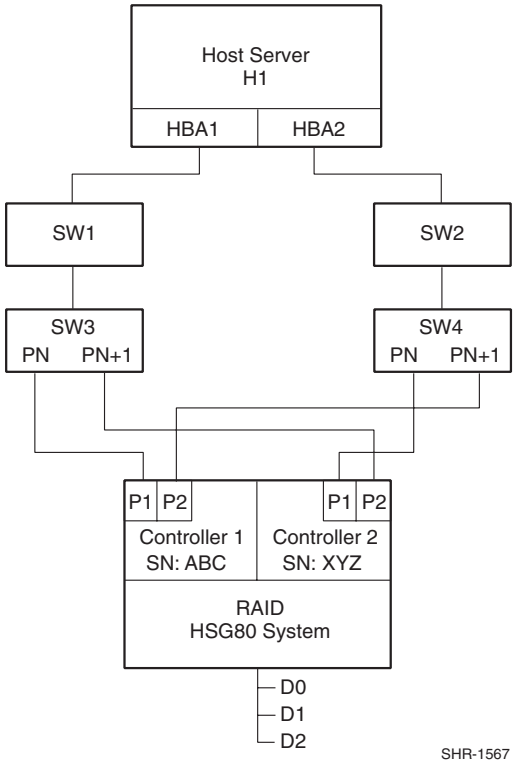
In most configurations, the same ALPAs will be assigned to the respective ports of the two RA8000/ESA12000 controllers. Since the ALPA to SCSI address mapping is fixed, this results in identical SCSI B-T-L values for the pair of P1 ports and the pair of P2 ports. The controller serial number information in the display provides a mechanism to correlate path information to a specific controller for maintenance purposes. It should also be noted that in the FC-AL topology, knowing the ALPA assignment for a particular controller port allows explicit path resolution to the port level.

Figure 2-2 also shows how the Secure Path Manager displays path information in the event that multiple hosts have access to the same device, such as would occur in a Microsoft Cluster for Windows NT environment.

Path Definition for Fibre Channel –Dual Switched Fabric

Figure 2-3 depicts a dual cascaded switch Fibre Channel topology and the resulting path connection information that would be displayed by Secure Path Manager. Fibre Channel adapters are referred to as HBAs and are named and numbered by Windows NT as SCSI ports. The rest of the SCSI address (except the LUN) is actually created within the Fibre Channel's miniport driver and is derived ultimately from Fibre Channel addressing information which is influenced by connections between the controller and the switch (specifically the switch domain and the switch port number). The LUN

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



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

Figure 2-3. Path Definition in a Secure Path Dual Cascaded Switch Fibre Channel Configuration

In Figure 2-3, devices found on SW3-Pn will be assigned the first available bus/target numbers - 1 and 0, respectively. (Note, the KGPSA miniport driver LP6NDS35 normally reserves Bus 0.) The LUN number is derived from the unit number assigned to the storageset within the controller using SWCC or CLI commands. The next port, SW3-Pn+1, gets the next sequential value of 1 – 1. (If there were additional storage systems connected, the address mapping

would continue incrementing Target numbers up to 31 at which point Bus 2 Target 0 would be assigned.)

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

Path Status

Secure Path displays the status of paths using two fields: Mode and State. Path mode may be one of Preferred, Alternate, Preferred-offline (pre-offline) or Alternate-Offline (alt-offline).

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

In addition, paths have a second attribute called *state* that may be one of the following: Active, Available or Failed. State is set automatically by RaiDisk and reflects current actual path status, which may deviate from user expectations as a result of path failures, etc.

- The Active state indicates that the associated path is currently servicing or is capable of servicing I/O to the storageset. When Load Distribution is enabled, multiple paths from the same host to the storageset may be in the Active state.
- Available state means that the associated path belongs to the set of redundant paths to the storageset that could be utilized during failover.
- Failed indicates that the path has encountered errors either during normal operation or as a result of Path Verification testing.

Chapter 6 provides more detailed discussion of path modes and states and provides illustrative examples of the effects of failovers, failbacks and user intervention.

Failover Operation

Failover is the operation performed by Secure Path when it detects that it can no longer communicate with a unit through its active path. Failover is done automatically upon detection of a selected set of error conditions. Secure Path normally performs path failover only when user I/O is active; it is possible that the Secure Path Manager will show some units with a common failed path in the failover state while other units appear to remain accessible through that path. Failover follows a certain hierarchy, conditioned by the state of Load Distribution. (Note that Secure Path does not change the mode of "Preferred" or "Alternate" paths in failover situations; this makes it easier for the user to restore the original path assignment(s) after effecting repair.)

- Load Distribution is *disabled*:

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

  If there is no "Alternate – Available" path on the same controller, Secure Path will attempt to move the device to an "Alternate – Available " path on the other controller. Secure Path will change only a single "Alternate-Available" path to "Alternate-Active" in accordance with its default path assignment algorithm.

- Load Distribution is *enabled*:

  Failover consists initially of marking the bad path "failed" which effectively removes it from the list of usable paths for the storageset.

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

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

The failover policy is optimized to minimize performance impact to the overall configuration. Other than Load Distribution as described above, there are no user-settable parameters that directly affect or modify Secure Path's failover policy.

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

Failback Options

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

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

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

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

Load Distribution

Load distribution, when enabled, allows multiple paths between a host and a specific storageset to be utilized in parallel for I/O. As was noted above, Fibre Channel interconnection schemes result in multiple paths between a host and each controller. I/O intended for storagesets connected to a given controller will be alternately dispatched through the set of appropriate paths, thus spreading the load across all components in the RAID storage system to maximize performance potential. Load distribution may not be used in Microsoft clusters or other environments that utilize device reservations as a lock mechanism since the RAID Array controllers in RA8000/ESA12000 enforce reservations on a per-port basis.

Load Distribution requires a Fibre Channel configuration that results in at least four unique paths from the host node to the storage system. While this can be accomplished with several different physical configurations, maximal performance potential is achieved when all four ports of the RAID storage

system are utilized. Since the RA7000/ESA10000 have only one port per controller, they do not normally benefit from Load Distribution.

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

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

Path Verification

Path Verification, when enabled, causes Secure Path to periodically test the viability of all paths to all storagesets for paths marked "Available", "Failed" or "Active". (Note, however, that paths that are in an "offline" mode are not tested under Path Verification.) Path Verification is useful for detecting failures that affect overall path redundancy before they impact failover capability. In essence, if a "Preferred" path fails path verification, failover occurs as described in the previous sections. If an "Alternate" path fails path verification, its state will change from "Available" to "Failed".

If a path currently marked "Failed" passes path verification, the path state will be set to "Available"; if auto-failback is enabled, the "Preferred" path(s) will become "Active".

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

Path Management Behavior Summary

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

Table 2-1
Path Management Behavior Summary

No I/O Distribution	**Startup**	1) Choose first path to controller on which LUN is online as **preferred active**, port does not matter – all other paths on both controllers marked **alternate available**. 2) If no online path is found, make any available path online and use as **preferred active** – all other paths marked **alternate available**
	Active Path Failure	1) Path marked **preferred (or alternate) failed** and fails to any other **alternate available** path on same controller, then other controller – port does not matter. **Alternate available** path used is marked **alternate active**. 2) Behavior is the same with I/O or background path verification. 3) If LUNs reserved, mark path **failed**, but do not fail to other path on non-owning node.
	Available Path Failure Path verification	1) Failed path marked **failed**. 2) Behavior is result of background path verification.
	Path Repaired	1) Path marked **available** 2) If autofailback is enabled, failback to **preferred** path from **available** path as regular “autofailback” function. 3) If LUNs reserved, mark path **available** but do not autofailback on non-owning node.

continued

Table 2-1
Path Management Behavior Summary *continued*

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

Chapter **3**

Fibre Channel Secure Path Installation

To install a new Secure Path fibre channel (FC) configuration, or to build Secure Path onto an existing fibre channel configuration, it is recommended that you first refer to the RA8000/ESA12000 High Availability (HA) Application Notes provided in the Secure Path software kit. This will help you become familiar with the high availability connection layout (FC devices and cabling) of the configuration you want to install or add.

The Application Notes present a topological layout of several HA options; provide part numbers and reference documentation, and discuss the performance considerations and restrictions that apply when Secure Path co-exists with Microsoft cluster software and FC hardware devices. At the time of this writing, two high availability application notes exist for Windows NT, which are as follows:

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

NOTE: For the most current Application Note information, access the Compaq web page at: **www.compaq.com/products/storageworks**

Components for RA8000/ESA12000 (FC) Secure Path Installation

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

Table 3-1
Secure Path (FC Installation) Prerequisites

Host Feature	Requirement
Platform	Intel
Operating System	Microsoft Windows NT Enterprise Edition, Version 4.0, SP5
Secure Path Software Kit	StorageWorks Secure Path v3.0 Enterprise Edition for Windows NT (QB-669AD-SA)
RAID Storage System(s)	StorageWorks dual-redundant RA8000/ ESA12000 (FC)
Solution Software Kit	StorageWorks Solution Software V8.5 for Windows NT (QB-65RAE-SA)
Host Bus Adapter(s) (and adapter driver)	Supported model for Windows NT Intel: StorageWorks KGPSA
FC Interconnect Hardware	FC hubs, switches, and connection hardware as required (Application Notes provide detailed equipment part numbers)

continued

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

Host Feature	Requirement
Service Tools	Appropriate tools to service the equipment
Technical Documentation	The reference guides for the RAID system, the host server and the Windows NT software supplement this installation guide.

Installing a New RA8000/ESA12000 Secure Path Configuration

This section provides the procedures to install and configure for a Secure Path topology starting with *new* fibre channel hardware components.

NOTE: In FC-Switch topologies, connect lower numbered controller ports numbers to lower numbered switch ports. This will simplify path identification as defined by the Secure Path Manager utility. For example, if port 1 of a controller is connected to switch port 3, controller port 2 should be connected to switch port 4 or higher. (Please reference Chapter 2 for a detailed discussion of path definition).

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

      HSG80> **set this_controller port_1_topology=offline**

      HSG80> **set other_controller port_1_topology=offline**

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

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

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

HSG80> **set this_controller port_1_topology=loop_hard**

HSG80> **set other_controller port_1_topology=loop_hard**

HSG80> **set this_controller port_2_topology=offline**

HSG80>**set other_controller port_2_topology=offline**

HSG80> **set this_controller port_2_al_pa=*n***

HSG80> **set other_controller port_2_al_pa=*n***

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

HSG80> **set this_controller port_2_topology=loop_hard**

HSG80>**set other_controller port_2_topology=loop_hard**

b. For Switched fabric environments, perform the following commands.

HSG80> **set this_controller port_1_topology=fabric**

HSG80> **set other_controller port_1_topology=fabric**

HSG80> **set this_controller port_2_topology=fabric**

HSG80>**set other_controller port_2_topology=fabric**

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

HSG80 > **set nofailover**

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

HSG80 > **set multibus copy=this**

The controllers will restart in multiple-bus mode.

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

HSG80 > **show this**

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

The controllers are now configured for multiple-bus operation.

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

IMPORTANT: Do not connect host bus adapters to any switches/hubs at this time.

5. Install Secure Path software on the Windows NT server(s).

   The Secure Path software is installed using the Secure Path setup wizard. To launch the Secure Path installation wizard, insert the *StorageWorks Secure Path Software V3.0 Enterprise Edition for Windows NT* CD into the CD-ROM driver. Please refer to Chapter 5, *Installing Secure Path Software* to complete the Secure Path software installation setup.

6. Shut down the server(s).

7. Connect all host bus adapters to the switches/hubs.

8. Reboot the server(s) one at a time, performing each step below. Repeat this step until all servers have been brought online.

   a. Using SWCC double-click on the desired controller icon in the main window. Choose the Connection tab to rename connections. Suggested connection names can be found in the application notes Storage Area Network Configurations for RA8000/ESA12000 on Windows NT – Intel or RA8000/ESA12000 FC-AL High Availability Configurations for Windows NT – Intel. Refer to the SWCC documentation if you need more information about managing connections.

   b. Set Unit Offsets so that each server or cluster requiring exclusive access to a set of LUNs has its own unique offset range. Note that each connection is restricted to a maximum of 8 LUNs.

   c. Create storagesets and provide unit attributes for LUNs on this server or cluster, including Preferred Path assignments using SWCC.

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

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

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

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

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

You have now completed the configuration procedures required to support the new Secure Path environment. To monitor and manage Secure Path activity using the StorageWorks Secure Path Manager, please refer to Chapter 6 of this guide.

Adding Secure Path to an Existing RA8000/ESA12000 Configuration

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

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

NOTE: In FC-Switch topologies, connect lower numbered controller ports to lower numbered switch ports. For example, if port 1 of a controller is connected to switch port 3, controller port 2 should be connected to switch port 4 or higher. This will simplify path identification as defined by the Secure Path Manager utility. (Please reference Chapter 2 for a detailed discussion of path definition).

1. Using the Command Line Interface (CLI), complete the following steps to configure the RAID system for Secure Path operation:

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

   HSG80 > **set nofailover**

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

   HSG80 > **set multibus copy=this**

   The controllers will restart in multiple-bus mode.

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

   HSG80 > **show this**

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

   The controllers are now configured for multiple-bus operation.

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

NOTES:

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

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

HSG80 > **show units**

Use the following commands to specify preferred_path for units:

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

- or -

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

c. Cycle power on the RAID cabinet for the preferred path settings to take effect.

2. Using the Command Line Interface (CLI), complete the following steps to configure the RAID system for Secure Path operation. For FC-AL configurations, perform step a; for switched fabric perform step b.

a. For FC-AL configurations, if the configuration entails utilizing additional ports on existing RAID system controllers, or if you are installing additional (new) RAID systems at this time, use SWCC to establish the Arbitrated Loop Physical Address (ALPA) assignments for all new controller ports by typing the following commands:

HSG80> **set this_controller port_1_topology=offline**

HSG80> **set other_controller port_1_topology=offline**

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

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

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

HSG80> **set this_controller port_1_topology=loop_hard**

HSG80> **set other_controller port_1_topology=loop_hard**

HSG80> **set this_controller port_2_topology=offline**

HSG80>**set other_controller port_2_topology=offline**

HSG80> **set this_controller port_2_al_pa=*n***

HSG80> **set other_controller port_2_al_pa=*n***

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

HSG80> **set this_controller port_2_topology=loop_hard**

HSG80>**set other_controller port_2_topology=loop_hard**

b. For switched fabric environments enter the following commands:

HSG80> **set this_controller port_1_topology=fabric**

HSG80> **set other_controller port_1_topology=fabric**

HSG80> **set this_controller port_2_topology=fabric**

HSG80>**set other_controller port_2_topology=fabric**

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

   NOTE: Do not connect new host bus adapters to the hubs/switches at this time.

5. Reboot server(s).
6. Referencing Chapter 1 of the *RAID Solution Software for Windows NT* installation reference guide, run the FC software setup (included with the RA8000/ESA12000 platform kit) on the host server(s) to set host bus adapter parameters.
7. Install Secure Path software on the Windows NT server(s).

   The Secure Path software is installed using the Secure Path setup wizard. To launch the Secure Path installation wizard, insert the *StorageWorks Secure Path Software V3.0 Enterprise Edition for Windows NT* CD into the CD-ROM drive. Please refer to Chapter 5, *Installing Secure Path Software* to complete the Secure Path software installation setup. If no additional paths are to the storagesets are being added at this time, you should skip to step 9.
8. Reboot the server(s) one at a time, performing each step below. Repeat this step until all servers have been brought online.

a) Using SWCC double-click on the desired controller icon in the main window. Choose the Connection tab to rename connections. Suggested connection names can be found in the application notes Storage Area Network Configurations for RA8000/ESA12000 on Windows NT – Intel or RA8000/ESA12000 FC-AL High Availability Configurations for Windows NT – Intel. Refer to the SWCC documentation if you need more information about managing connections.

b) Set Unit Offsets so that each server or cluster requiring exclusive access to a set of LUNs has its own unique offset range. Note that each connection is restricted to a maximum of 8 LUNs.

c) Create any additional storagesets and/or modify unit attributes for LUNs on this server or cluster, including Preferred Path assignments using SWCC. Note that Unit Number assignments must be made based on the Unit Offset numbers created in step 8b and should be consecutive from the base offset number.

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

9. Reboot server(s).

10. Verify the Secure Path configuration.

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

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

Chapter **4**

Secure Path (SCSI) Installation

This chapter provides the procedures for installing and configuring new Secure Path components into an existing RA7000/ESA10000 (SCSI) RAID storage configuration. These procedures require that you have already installed your RAID system in a single host/single path or dual host/single path configuration. And, that you have created storagesets on the RAID system using CLI/SWCC, and have partitioned and formatted these drives with the Windows NT Disk Administrator.

Secure Path (SCSI Installation) Pre-requisites

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

Table 4-1
Secure Path (SCSI Installation) Prerequisites

Host Feature	Requirement
Platform	Intel
Operating System	Microsoft Windows NT Enterprise Edition, Version 4.0, SP5
Secure Path Software Kit	StorageWorks Secure Path v3.0 Enterprise Edition for Windows NT (QB-669AD-SA)
RAID Storage System(s)	StorageWorks dual-redundant RA7000/ESA10000 (UltraSCSI)
Solution Platform Kit	StorageWorks HSZ70 Solution Software for Windows NT –Intel (QB-5SBAE-SA)
Host Bus Adapter(s) (and adapter driver)	Adaptec AHA-2944UW
Interconnect Hardware	As required
RAID Hardware	Cables supplied with the RAID system
Service Tools	Appropriate tools to service your equipment
Technical Documentation	The reference guides for your RAID system, the host server and the Windows NT software supplement this installation guide.
Configuration-Specific SCSI Interconnect Kit	SWXKT-EA –UltraSCSI Hub Cluster RAID Kit SWXKT-FA –RAID SCSI Connection Kit SWXKT-DF –Cluster RAID Connection Kit

Prepare the RAID System(s) for Secure Path Operation

This section describes how to prepare your RAID system(s) for a Secure Path environment, depending on whether you are adding Secure Path capability to an *existing* (in use) SCSI RAID configuration, or the Secure Path installation includes a *new* SCSI RAID system.

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

Preparing *Existing* RAID System(s) for Secure Path Operation

For each RAID currently being used in a production environment that you plan to reconfigure for Secure Path operation, follow normal procedures to backup the data stored on your RAID system(s).

Preparing *New* RAID System(s) for Secure Path Operation

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

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

Examine the Current Single Path

The next step in preparing a RAID system for Secure Path is to ensure that the current (existing) single path configuration conforms to Secure Path requirements. Confirm that the existing storage infrastructure is robust as follows:

1. Verify that there is a serial connection to the storage system and that you can communicate to it via SWCC or the CLI.
2. Check the NT event log viewer and determine that there are no error events reported by the host adapter or HszDisk.
3. Verify that the Windows NT system (boot) disk is not part of the storage system.
4. Verify that the server has the TCP/IP protocol installed and that the server is available on the network by pinging it.

Secure Path (SCSI) Installation

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

Summary

Configuring Secure Path hardware components consists of the following tasks that must be performed in sequence, as described in this chapter.

- Prepare the additional SCSI host bus adapter(s).
- Install the additional SCSI host bus adapter(s) into the server(s)
- Cable the SCSI hardware components
- Verify the Secure Path hardware configuration

Preparing Additional SCSI Host Bus Adapter(s)

Secure Path installation requires that at least one additional SCSI host bus adapter (Adaptec AHA2944UW) be installed into the host server. Prior to installing a SCSI host bus adapter, prepare it for Secure Path operation as follows:

1. Set/Verify SCSI Host Adapter Termination
2. Disable SCSI Bus Reset
3. Disable SCSI Host Adapter BIOS
4. Set Start Unit to “NO”

Setting Up SCSI Host Bus Adapters

Refer to the documentation supplied with your SCSI host bus adapter to configure the parameters below. Adapter settings must be identical for each host adapter.

1. Termination is **enabled** unless you are using Y-cables with external termination. If you are using Y-cables with external termination then you must **disable** termination on the host bus adapter.

2. SCSI bus resets following board initialization (power-on reset) are **disabled.**
3. SCSI host bus adapter BIOS is **disabled**.

Installing the Host Bus Adapter(s)

Follow the adapter vendor's recommended procedure to install the additional SCSI host bus adapter(s) into your server(s).

Cabling and Termination

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

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

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

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

1. Install the host bus adapter in the server.

2. Remove the link cable connecting both HSZ70 RAID controllers in the system.

3. Connect a terminator (H8863-AA) to the remaining tri-link connector of the controller that is currently connected to the host server.

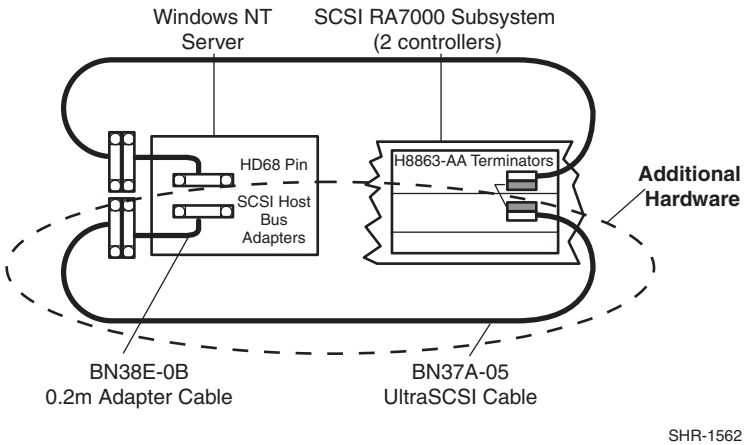


Figure 4-1. Secure Path Hardware Interconnect – SCSI Single Server

NOTE: In Figure 4-1, notice that the link between the two RAID controller boards has been removed, and that both busses are terminated on the controller.

4. Attach end of the UltraSCSI cable (BN37A-05) to the tri-link connector on the controller in the RAID system that is not currently connected to the host server.

5. Connect end of the .2M adapter cable (BN38-E-0B) to the available end of the UltraSCSI cable.

6. Attach the other end of the .2M adapter cable to the available SCSI host adapter board resident in the host server.

7. Verify that the terminator (H8863-AA) pre-existing in the newly-cabled controller is firmly attached into its tri-link connector.

8. Reboot the host server.

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

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

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

1. Install a host bus adapter into each server.

2. Remove the link cable interconnecting both HSZ70 RAID controllers in the storage system.

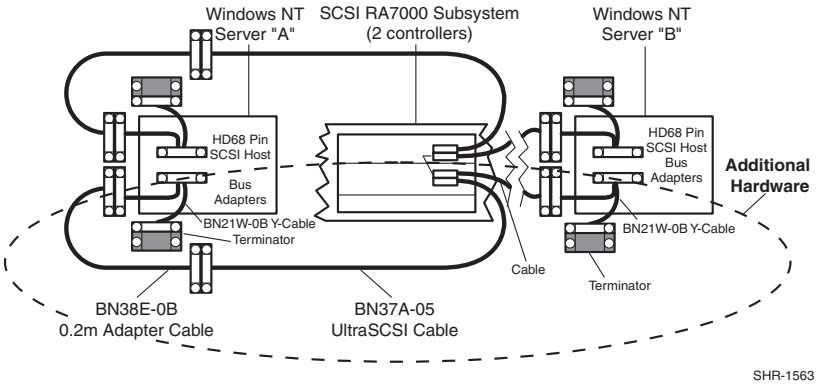


Figure 4-2. Secure Path Hardware Interconnect – SCSI Cluster Y-Cable

3. Move one of the existing VHDCI cables from the bottom controller to the top controller. Both connectors on the bottom controller should now be unused.

4. Attach Y-cables to each of the new host bus adapters, one new adapter in each server.

5. Attach SCSI terminators to one end of each Y-cable.

6. Attach the (compatible) end of the .2M adapter cable (BN38E-0B) to the available end of the Y-cable of one server, and extend it to the bottom controller using the 5 meter VHDCI cable (BN37A-05)

7. Attach the VHDCI/HD68 5 meter cable between the remaining Y-cable and the bottom controller.

8. Reboot the host servers.

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

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

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

1. Install the host bus adapter in the servers.

2. Remove the link cable interconnecting both HSZ70 RAID controllers in the storage system.

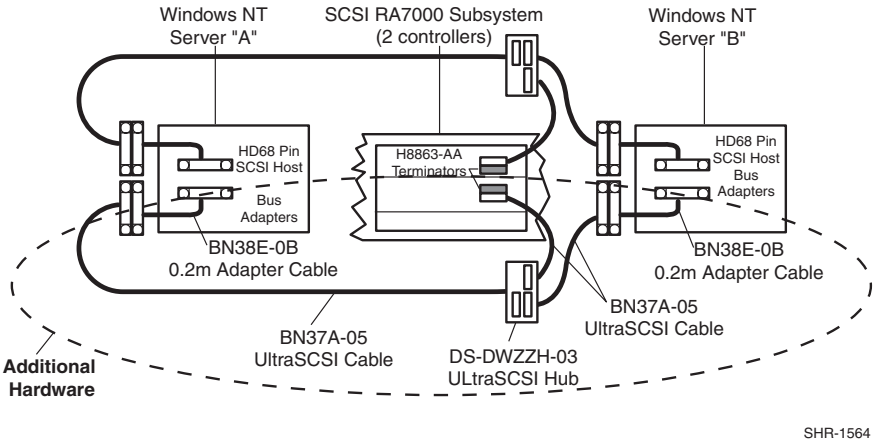


Figure 4-3. Secure Path Hardware Interconnect – SCSI Cluster Hub

3. Install a VHDCI terminator on the both controllers (one already has a terminator installed)

4. Attach the (compatible) end of the .2M adapter cable (BN38E-0B) to the host bus adapters, and extend it to a SCSI hub using the 5 meter VHDCI cable (BN37A-05)

5. Connect the remaining port of the 3 port SCSI hub to the RAID Array controller.
6. Reboot the host servers.

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

Verify the Secure Path Hardware Configuration

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

Chapter 5

Installing Secure Path Software

Components of the Secure Path Software

Secure Path for Windows NT consists of two software components that are installed individually, as described in this section. The components are:

- Server software (Raidisk filter driver, Hszdisk driver and SecurePathAgent)
- Client software (Secure Path Manager GUI)

Installing the Server Software

NOTE: The Secure Path Server software must be installed on the same Windows NT host system to which the RAID storage system is connected. TCP/IP must also be installed on this same host system.

Install the Secure Path Server software as follows:

1. Insert the *StorageWorks Secure Path Software (v3.0) for Windows NT* CD into your CD-ROM drive.
2. If you have CD Autorun enabled on your server, the Secure Path setup program will start automatically. Otherwise, Choose "Run" from the START menu and enter the following command:

   ***drive_letter*:\spinstal\setup.exe**

   where: *drive_letter* is that of the CD-ROM.

When the setup starts, choose the destination path, then choose the "Secure Path Server Install" option, which will install the required drivers and agent.

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

There are many ways to configure TCP/IP on your network. They include:

- host files on servers and clients
- DNS, with NetBios using DNS resolution.

Check with your system administrator to assure proper network configuration.

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

Installing the Client Software

NOTE: Secure Path Client software can be installed on the same Windows NT host system as the Server software, and/or it can be installed on any Windows NT (TCP/IP-capable) workstation.

Install the Secure Path Client software as follows:

1. Insert the *StorageWorks Secure Path Software (v3.0) for Windows NT* CD in your CD-ROM drive.
2. If you have CD Autorun enabled on your server, the Secure Path setup program will start automatically. Otherwise, Choose "Run" from the START menu and enter the following command:

   ***drive_letter*:\spinstal\setup.exe**

   where: *drive_letter* is that of your CD-ROM

   When the setup starts, choose the destination folder, then choose the "Secure Path Client Install" option, which will install the Secure Path Manager software.

Chapter 6

Managing Secure Path

About Secure Path Manager

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

SPM is installed automatically when you select either the Client or Client and Server options during Secure Path Setup (refer to Chapter 5). Use the Client and Server option when you wish to manage Secure Path from a server that is directly connected to the storage system. Use the Client only option when you wish to manage a Secure Path installation remotely from a PC running Windows NT on your network.

Please refer to Chapter 2, *Technical Description* for detailed information regarding Secure Path configuration applications and storage path identification in a high availability environment.

Launching Secure Path Manager

To invoke the SPM, reference Figure 6-1 and proceed as follows:

1. From the START menu, select the Programs\ StorageWorks\SecurePath Mgr submenu.
2. Click on the Secure Path Manager application icon.

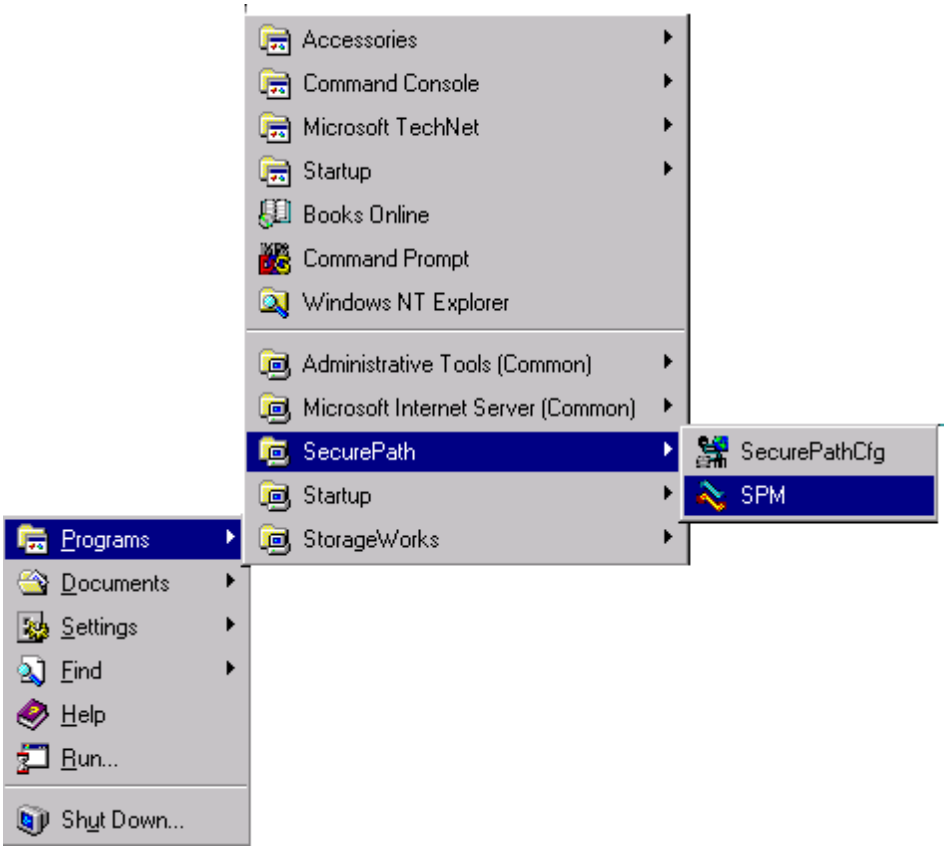


Figure 6-1. Launching the Secure Path Manager

Logging-On To Secure Path Manager

Defining SPM Storage Profiles

SPM displays a *storage-centric* view of Secure Path managed RAID storage resources. This means that all Secure Path protected RAID storage systems that are common to a given host or set of hosts are presented in an SPM display. The host or set of hosts that share these RAID storage systems are those you entered during SPM login, when you define a storage profile.

You define a storage profile from the login window when SPM is first launched. To create a non-clustered host profile, start by entering a host name or set of host names in the "Host-Cluster Names" field. To create a clustered-host profile (Figure 6-2), enter a host name or set of host names with each followed by a "-your clustername", to identify cluster membership.

An instance of SPM is capable of managing multiple non-clustered hosts sharing one or more RAID storage systems or multiple sets of clustered-hosts sharing one or more RAID storage systems. More than one instance of SPM must be used to manage installations that include a mix of non-clustered and clustered-hosts.

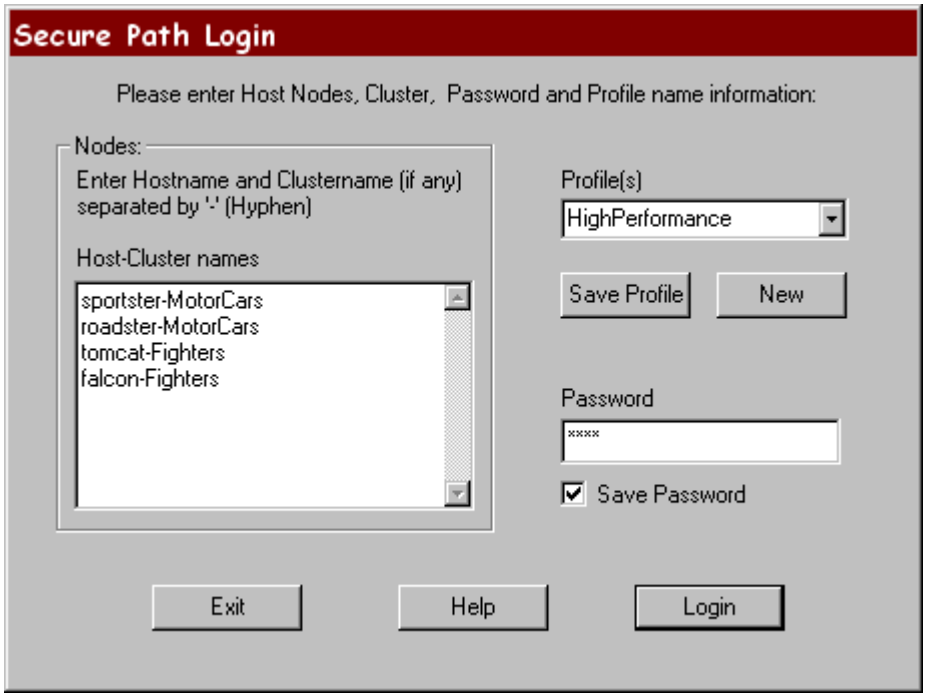


Figure 6-2. SPM Login Window with a Clustered Host Storage Profile

After you have added all the host names to your storage profile enter the connection password in the "Password" field. This is the password that you defined for the Secure Path Agent during Secure Path Setup or when you run the Secure Path Agent Configuration utility after installation. This password will be used by SPM to establish a network connection with the Secure Path host(s). Note that for storage profiles including more than one host, the connection password must be the same on each of the Secure Path host(s). Check "Save Password" if you want SPM to use the saved password automatically each time you login with this storage profile.

Saving an SPM Storage Profile

Once you have defined a storage profile, enter a name for it in the "Profile(s)" field. Save the profile by clicking the "Save Profile" button.

Creating A New SPM Storage Profile

To create additional SPM storage profiles, click the “New” button, add host name/s in the “Host-Cluster Names” field, enter a profile name in the “Profile(s)” field and click the “Save Profile” button.

Selecting an Existing SPM Storage Profile

To choose an existing SPM storage profile use the pull down arrow on the “Profile(s)” box to find and select the profile. If you did not choose to save the password when you originally created the profile, enter the password in the “Password” field and click the “Login” button.

Editing an Existing SPM Storage Profile

To edit an existing storage profile use the pull down arrow on the “Profile(s)” box to find and select the profile to be edited. Make the desired changes to the profile and click the “Save Profile” button.

Changing the Secure Path Agent Password

To change the Secure Path Agent’s password you need to run the Secure Path Agent Configuration utility located in the Secure Path program folder from the Start Menu. Once you have changed an agent’s client (SPM) access list and/or password using the Configuration utility you must stop and restart the agent using the Windows NT Services Applet located in Control Panel. Find and select the Secure Path Agent in the list of services and click the “Stop” button (Figure 6-3). Once the agent has stopped, select Secure Path Agent again and click the “Start” button. The agent will now restart and update its client and/or password database. Make sure that you do this for each of the hosts in an SPM storage profile.

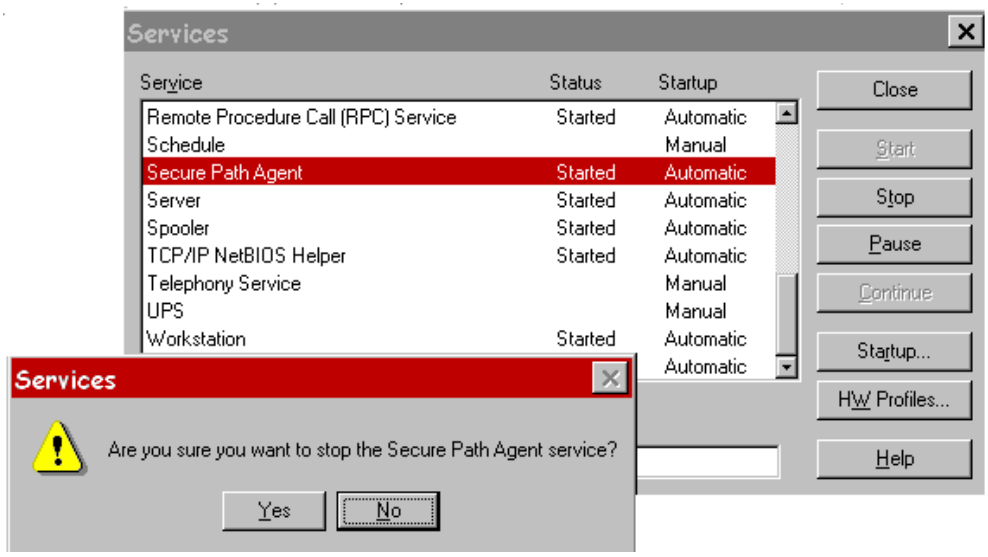


Figure 6-3. Stopping the Secure Path Agent

Troubleshooting Connection Problems

If you experience problems attempting to login to SPM, refer to Chapter 8, *Troubleshooting Secure Path Connection Problems.*

Monitoring Host Connections

SPM monitors the connection status for each active host that is a member of the current storage profile. As shown in Figure 6-4, a server icon is displayed for each host in the window frame located immediately below the tool bar. The host's name is listed above the icon and a cluster name is listed below if it is a member of a cluster.

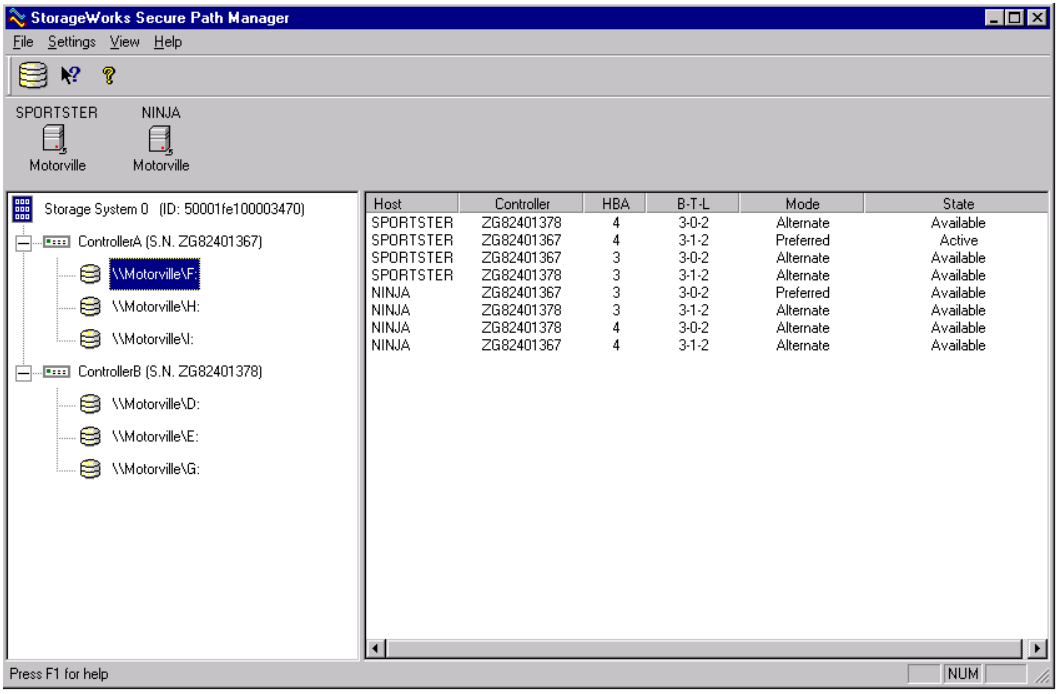


Figure 6-4. Host Connection Monitor

SPM monitors its connection with each member of a storage profile and will indicate a loss of connection to a particular host with a red “X”. Figure 6-5 below shows that SPM has lost connection to the Motorville cluster member Sportster.

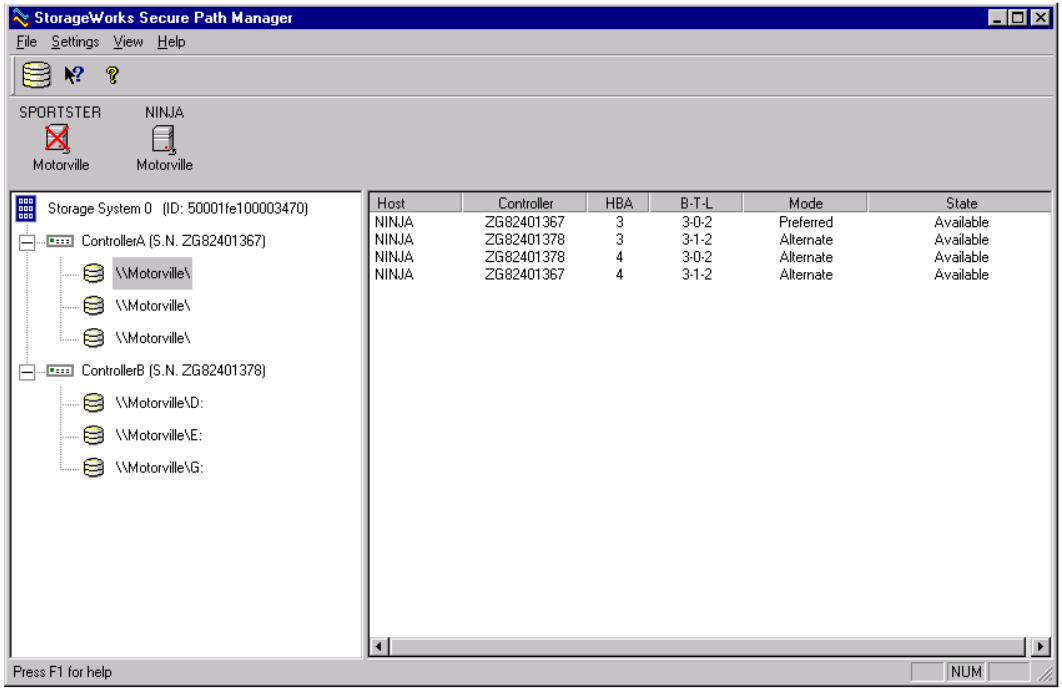


Figure 6-5. Lost Host Connection Icon

Responding To A Lost Host Connection

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

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

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

Setting Storage Profile Properties

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

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

Storage System View

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

Storage Systems and Controllers

- **Storage System ID** - Each RAID Array storage system is identified by a unique 64-bit value. For RA7000/ESA10000, the Storage System ID is generated by Secure Path and is derived from the controller serial numbers. If an RA7000/ESA10000 controller is swapped, the Storage System ID will change. For an RA8000/ESA12000, the Storage System ID is determined at time of manufacture and stored in controller VRAM. The Storage System ID for RA8000/ESA12000 remains constant for the life of the RAID storage system.
- **Controller Serial Number** - The individual controllers of a RAID Array storage system are identified by a unique 10 place alphanumeric value assigned during controller manufacture.

RAID Array Storagesets

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

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

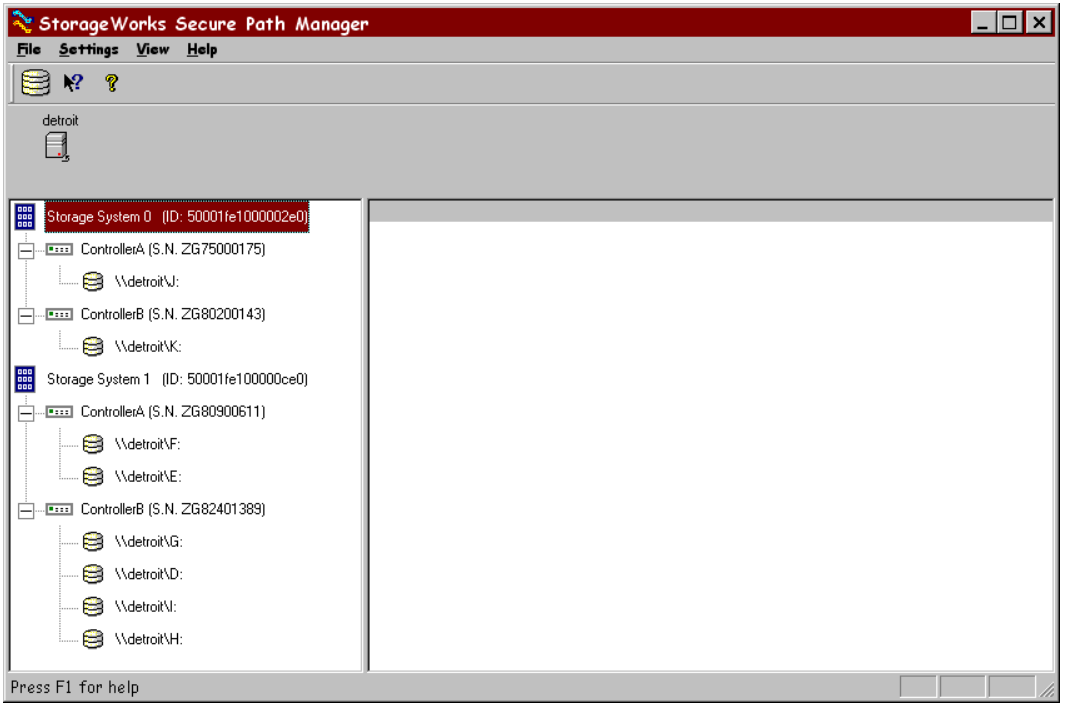


Figure 6-6. SPM Single Host Storage Profile –Storage System View

Physical Path View

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

- **Host** – is the Secure Path host system, which has an established access path to the storageset.
- **Controller** – is the RAID storage system controller servicing the path.
- **HBA** – represents the physical port number of the Host Bus Adapter servicing the path. The HBA is a relative number determined by Windows NT's order of discovery for adapters on that host.
- **B-T-L** – the physical Bus, Target, and LUN number describing the path address for the storageset.

- **Mode** - A user selectable parameter that specifies path behavior during nominal and failure conditions. Path mode may be set to Preferred, Alternate, Pre-Offline (Preferred and Offline), or Alt-Offline (Alternate and Offline).
- **State** – A set of attributes that describe the current operational condition of the path. Paths may exist in Active, Failed, or Available states.

The SPM screen (Figure 6-7), shows a simple single host configuration, with the host Detroit attached to two Secure Path protected RAID storage systems. Browsing on the controllers of Storage System 1 shows that two storagesets are owned by controller A and four storagesets are owned by controller B.

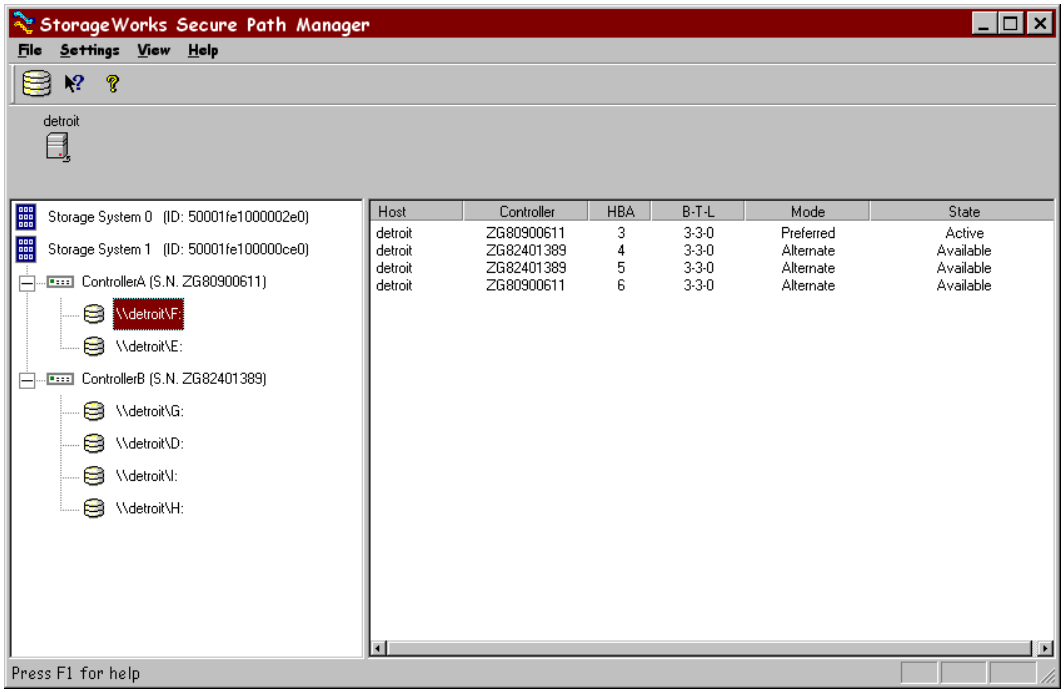


Figure 6-7. SPM Single Host Storage Profile – Physical Path View

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

The display information in this example shows that there are four paths configured from host Detroit to drive F. One of the paths accesses the

storageset at Bus 3, Target 3, and LUN 0 through the Host Bus Adapter (HBA) at Port 3, one through Port 4, another Port 5, and the last through Port 6.

Information for the first path indicates that it is in a Preferred mode and Active state. The initial starting state is derived from the controller's preferred path attribute or the last owning controller. The Preferred mode is selected by a user for a given path, to specify its use for all I/O operations during normal conditions. A path with a Preferred mode that is in the Active state is one that is currently being used for access to a storageset under normal operating conditions.

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

Notice that the controller serial number displayed for the Preferred path is the same as the one shown in the Storage System view for the controller owning drive F. Also, notice that two of the paths in the Available state have a different serial number than that of the Preferred mode path, indicating that they are providing standby access through the other controller. This means that should the controller currently servicing the Preferred path completely fail, one or more of the paths on the surviving controller will transition to the Preferred state, depending on whether or not Load Distribution has been enabled.

Polling Interval and Display Refresh

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

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

Manipulating Storagesets and Paths

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

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

Moving A Storageset

Choose *Move a Storageset* when you want to change the ownership from the current RAID Array controller to the other. This action is useful if you need to balance I/O loading across controllers or to manually return a failed-over storageset to its Preferred path when Auto-Failback has been disabled. There are two methods available to move a storageset. Click on the drive to highlight it in the storage system view, then either drag the drive to the other controller or right click to select the "Move To Other Controller" action.

Making A Path Alternate

Choose *Make a Path Alternate* when you have Load Distribution enabled and you want to disable I/O operations to one or more paths. To make a path Alternate click on the Preferred path you wish to change and then right click to select the "Make Alternate" action.

Making A Preferred Path

Choose *Make a Path Preferred* when you have Load Distribution enabled and you want to re-enable I/O operations to a path that you have previously disabled using "Make Alternate". To make a path Preferred click on the Alternate path you wish to change and then right click to select the "Make Preferred" action.

Changing A Preferred Path

Choose *Change a Preferred Path* when Load Distribution is disabled; there are multiple paths available to a storageset on the same controller and you wish to select a new Preferred path for normal I/O operations. To change a Preferred path, click on the Alternate path you wish to change to Preferred, and then right click to select the "Change Preferred" action.

Making A Path Offline

Choose *Make a Path Offline* when you want to prevent that path from being used for any I/O operations under any circumstances. For instance, use the Offline mode when you need to replace or work on a storage interconnect component. To make a path Offline, click on a Preferred or Alternate path and then right click to select the "Make Offline" action. If the path was an Alternate, its mode will change to "Alt-Offline". If the path was Preferred, its mode will change to "Pre-Offline".

Making A Path Online

Choose *Make a Path Online* when you want to return a path that is currently in the "Alt-Offline" or "Pre-Offline" mode to its original mode. To make a path online, click on a path in the "Alt-Offline" or "Alt-Online" mode and then right click to select the "Make Online" action. If the path was "Alt-Online", its mode will change to "Alternate". If the path was "Pre-Offline", its path will change to "Preferred".

Verifying A Path

Choose *Verify a Path* when you want SPM to determine the current state of a path. To Verify a path, click on the path and then right click to select the "Verify Path" action. SPM will generate a pop-up message when the verification completes to indicate the result of the operation. No state change will occur as a result of this operation.

Repairing A Path

Choose *Repair a Path* when you want SPM to restore access to a failed path after the problem has been corrected. To Repair a path, click on a path in the FAILED state and then right click to select the "Repair Path" action. If the

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

Detecting and Identifying Path and Controller Failures

SPM periodically monitors the status of all systems in your storage profile at a rate determined by the Polling Interval. To indicate failures, icons are used in the Storage System view and path states are set to FAILED in the Physical Path view. In addition, failover events are logged by the RaiDisk driver in the Windows NT Event Viewer. The Secure Path Agent will also notify StorageWorks Command Console clients immediately when a fault is detected.

It is suggested that you routinely monitor SPM status to check for the occurrence of failover events that might compromise either the performance or availability of storage resources. For example, if you use Load Distribution to enhance the performance of your storage resources, this capability may be diminished if one or more of your Active paths are lost due to component failure. Also, availability is compromised if your configuration includes only two configured paths to a storageset and one is lost due to component failure. Secure Path will be unable to failover to a redundant path should a subsequent fault occur in this situation.

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

Detecting Path Failures

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

Storage System Path Failure Detected

The icon shown in Figure 6-8 indicates that a failure of at least one, but not all paths to that RAID Array storage system was detected by Secure Path. Browse the storage system to determine the affected controller and storagesets.

Figure 6-8. Storage System Path Failure Detected

Storage Controller Path Failure Detected

The icon shown in Figure 6-9 indicates that a failure of at least one, but not all paths to that storage controller was detected by Secure Path. Browse the storage controller to determine the affected storageset(s).

Figure 6-9. Controller Path Failure Detected

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

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

Storageset Path Failure Detected

The icon shown in Figure 6-10 indicates that a failure of at least one, but not all paths to that storageset was detected by Secure Path. Click on the storageset to highlight it and examine the Physical Path view information to determine the specific nature of the path failure.

Figure 6-10. Storageset Path Failure Detected

Total Path Failures

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

Figure 6-11. Storage System Failure Detected

Figure 6-12. Storage Controller Failure Detected

Figure 6-13. Storageset Failure Detected

Identifying Path Failovers

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

- Was I/O active on the affected storageset?

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

- Is Path Verification enabled?

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

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

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

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

Identifying Controller Failovers

A RAID Array controller failure will cause Secure Path to change the ownership of a given storageset to the surviving controller. Failover will occur only for those storagesets with active I/O operations. If you suspect that a

controller failover has occurred use the Path Verification feature to check the viability of all configured paths. Although you may enable it at anytime, Path Verification will require approximately two minutes per storageset to verify the integrity of all paths in the storage profile.

The Path Verification diagnostics will identify the specific failing controller in the Storage System view. Check for the failed storage controller icon shown in Figure 6-12. SPM will show that all storagesets previously on this controller have been failed-over to the surviving controller. Because all of the Alternate paths to the faulty controller have transitioned to the FAILED state as a result of Path Verification, storageset path failure icons will be displayed for each storageset on the surviving controller.

Responding to Failover Events

When investigating possible problems with failovers, consider the following:

- Are there additional Available paths remaining to the storageset or has this failure totally eliminated the ability to survive any subsequent failures?
- If you have Load Distribution enabled, are other paths and/or controllers suffering degraded performance due to the increased load placed on the remaining paths?
- What caused the failure?

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

Using SPM with MSCS and OPS Clusters

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

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

Microsoft Cluster Server Environments

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

Oracle Parallel Server Environments

Oracle Parallel Server allows multiple instances on different hosts to mount and access the same database files. Oracle Parallel Server uses a Distributed Lock Management mechanism to synchronize and control attempts by two or more hosts to modify the same information simultaneously. In an OPS cluster environment all hosts effectively "own" all shared storagesets all the time. This means that when you view a storageset from the Physical Path view each member of the OPS cluster will have a path to that drive in the Preferred mode and Active state.

Chapter 7

Using StorageWorks Secure Path with SWCC

Introduction

This chapter describes how to use Secure Path v3.0 in conjunction with StorageWorks Command console (SWCC).

StorageWorks Command Console is a windows-style graphical user interface that uses standard Windows navigation, command selection and navigation features. Folders are used to arrange Secure Path managed storage systems and non-Secure Path managed storage systems.

The SWCC Navigation Window (Figure 7-1) provides a list of all the host computers and storage systems to which SWCC is connected. You can use the Navigation Window to monitor storage systems for failures. SWCC will monitor your network connection and storage system and report status by changing the icons in the Navigation Window.

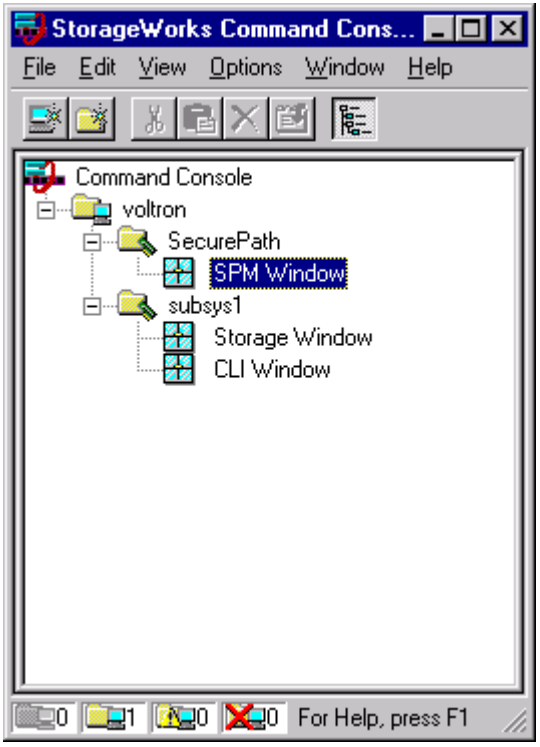


Figure 7-1. SWCC Navigation Window

Adding a Secure Path System to the Network

1. From the File menu, click *Add System* (Figure 7-2).
2. Enter a Domain Name Service (DNS) name or the IP address in the *Host name or TCP/IP address:* text box (shown in Figure 7-3) and click *Apply*. After you click *Apply*, Client adds an icon in the Navigation Window for the host running the Secure Path Agent. The example in Figure 7-4 shows that *voltron* is the host running the Secure Path Agent.
3. When the second *Add System* dialog box appears, click the *Close* button.

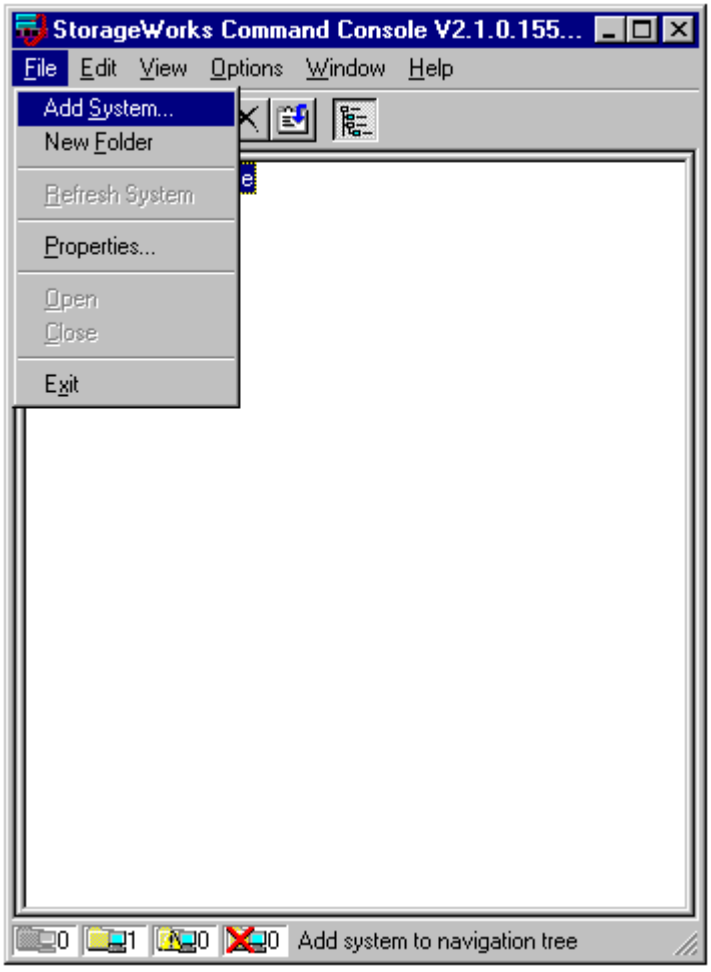


Figure 7-2. Adding a System

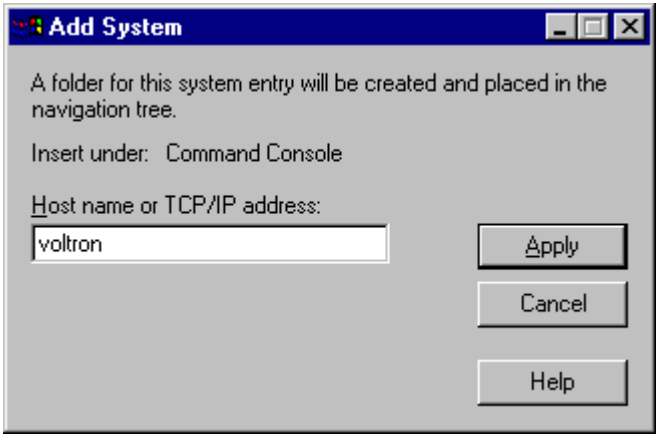


Figure 7-3. Add System Dialogue Box

Figure 7-4. System 'Voltron" Added to the Navigation Window

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

- Host Folder – which has the host name, shown as *voltron* in the example
- Storage System Folder – shown as *Secure Path* in the example
- SPM Window – The SPM window does not support the launching of Secure Path Manager (SPM). To launch SPM, select the SPM icon from START/Program/SecurePath menu. Note that attempting to launch SPM from SWCC Navigation Window will result in following error message:

Using SWCC to Monitor the Secure Path System

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

Controller Folders

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

Table 7-1
Controller Folder States

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

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

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

Chapter **8**

Troubleshooting Secure Path Connection Problems

This chapter describes general network configuration issues that might affect the ability of the Secure Path Client and Agent to establish connection.

Client/Agent Considerations

- Add each client's NetBIOS name or Fully Qualified Domain Name (FQDN) to the agent's list of authorized clients using the Agent Configuration utility, and set the password in the password dialog box. Once you've made the modifications, Stop and Restart the Secure Path Agent to update the database using the Services applet from Control Panel.
- Make sure that you use the same name type, either NetBIOS or FQDN, during Secure Path client login that you have entered in the agent's database.
- Each name you use must be mapped to its network IP address using a HOSTS file (static text file with either NetBIOS or FQDN mapped to IP,) the Windows Internet Naming Service (WINS with a NetBIOS name), or by the Domain Name System (DNS with a Fully Qualified Domain Name.) See network considerations below for more information.
- In cluster configurations make sure that the password you choose is common for both agents in the cluster.

- Secure Path does not use Windows NT domain authentication to authorize clients. Client authentication is handled for each agent using name-to-IP address resolution and password verification from the Secure Path configuration database.

Network Considerations

- Client names up to 15 letters without a dot (".") can be resolved by NetBIOS broadcast resolution as long as the client and agent nodes are configured on the same subnet. If the client and agent are located on different subnets then you must use either the LMHOSTs file, HOSTs file, WINS, or DNS to resolve the address.
- If you use the LMHOSTs file make sure that the "Enable LMHOSTs Lookup" box is checked in the TCP/IP protocol properties of the client system. On the client system you must enter the NETBIOS name and the IP address of the agent you wish to connect with in the LMHOST file and save it. Click the "Import LMHOSTS" button to specify the location of the LMHOST file. The LMHOSTs and HOSTs files are normally located in the \system32\drivers\etc subdirectory. Finally, from a command prompt issue the "NBTSTAT -R" command to purge and reload the remote name table.
- Client names that exceed 15 letters or with a dot require an entry for that name in the HOSTS file or resolution by a DNS server. It is also possible to have DNS resolve NetBIOS names as long as the DNS server is updated with the appropriate information. Make sure that you have checked the "Enable DNS for Windows Resolution" box in the TCP/IP protocol properties of the client system.
- If you are using DNS for host name-to-IP resolution, then the DNS database on the DNS server must be updated with the appropriate information.
- For best network connection results, it is recommended that you use Fully Qualified Domain Names with DNS.
- For production environments, where management and security are a concern, it is recommended that fully qualified names be used with DNS name resolution.
- For test and evaluation environments it is usually easier to simply add the server's name to the client's HOSTS file and the client's name to the server's HOST file.
- Make sure that you can ping the Secure Path host both locally and from a remote host using the host name, not the IP address.

Appendix A

Glossary

StorageWorks Secure Path Terminology

Bus For parallel SCSI configurations, the bus is a number assigned to the physical interconnect(s) emitted by a host bus adapter.

For Fibre Channel configurations, host bus adapters may utilize multiple bus numbers as an artificial method of expanding bus address space.

Controller The hardware device that facilitates communication between a host and one or more LUNs organized as an array. The HSZ70 and HSG80 are array controllers supported for use with Secure Path. Each controller in an HSZ70 or HSG80 RAID system is identified by a unique serial number, which is displayed next to the controller icons by Secure Path Manager. Secure Path Manager identifies a pair of controllers configured in multiple-bus mode by a unique 64-bit identifier that is displayed next to the subsystem icon.

HBA The I/O device (Host Bus Adapter) which serves as the interface connecting a host system to the SCSI bus or SAN (Storage Area Network). Host bus adapters are assigned a relative port number by the Windows NT operating system according to order of discovery (see Port).

Host The computer system on which the Secure Path server software (RaiDisk driver and Agent service) is running.

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

Mode User selectable parameters that specify path behavior during nominal and failure conditions. Paths may be set to one of the following modes:

- **Preferred** - indicates the desired I/O path(s). When Load Distribution is enabled I/O is distributed to a LUN using all available preferred paths according to a round-robin policy. When Path Verification is enabled all preferred paths would be verified.
- **Alternate -** indicates a path is used only for device access once all Primary Paths to the device have failed. Paths in this mode participate in path-verification, if enabled.
- **Offline -** indicates a path that will not be used for I/O to a LUN. The Offline mode is logically or'd with one of the other two path modes.

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

Port The relative number of a host bus adapter. A specific port number is determined according to its order of discovery by the Windows NT operating system and includes SCSI, Fibre Channel, and IDE adapter types.

Reduced Mode The condition of a system where one or more *redundant* components fail, but the system is operational.

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

- **Active** indicates a path that is currently servicing I/O requests.
- **Failed** indicates a path that is disabled and not actively servicing I/O requests.
- **Available** indicates a path that is neither Active nor Failed.
- **Remote** indicates a path that connects to a remote member of a PPRC (Point-to-Point Remote Copy) configuration. Remote state may be logically or'd with any of the other states.

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

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

Appendix ***B***

Removing StorageWorks Secure Path Software

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

How to Remove StorageWorks Secure Path Software

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

1. Establish a serial connection to the storage system.
2. At the RAID storage system prompt, enter the following command:

   HSZ70> **set nomultibus**

   The other controller will shutdown. Momentarily depress the restart button on the controller's front panel to restart the controller. Wait for the controller to restart, then enter:

   HSZ70> **set failover copy = this**

The controllers will configure for dual-redundant operation.

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

The Secure Path software removal process is complete.

Appendix C

Valid ALPA Settings

Table C-1 lists the valid ALPA settings for hard addressing the fibre channel arbitrated loop. For controller ports, select from ALPA addresses 0x71 and above. The grayed-out addresses are reserved.

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

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

continued

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

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

Index

H

I

K

L

M

O

P

R

S

T

U

V

W

Y