COMPAQ SANworks

Secure Path for Windows 2000 on RAID Array 4000/4100 Version 3.1

Installation and Reference Guide

First Edition (August, 2000)
Part Number AA-RN0DA-TE
Compaq Computer Corporation

Compaq SANworks Secure Path for Windows 2000 on RAID Array 4000/4100 Installation and Reference Guide Version 3.1
First Edition (August, 2000)
Part Number AA-RN0DA-TE

Contents

Chapter 3
Installing Secure Path

Chapter 4
Managing Secure Path

List of Figures

List of Tables

About This Guide

This guide contains step-by-step instructions for installation and reference information 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.
Emphasis or variable user input	Items for emphasis or variable user inputs appear in 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 installation.
- 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

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

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

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

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

Compaq Website

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

Compaq Authorized Reseller

For the name of your nearest Compaq Authorized Reseller:

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

Chapter 1

Theory of Operation

Overview

Compaq *SANworks Secure Path for Windows 2000 on RAID Array 4000/4100, Version 3.1* is a high-availability software product that manages and maintains continuous data access to the following Compaq StorageWorks storage systems:

- StorageWorks Fibre Channel RAID Array 4000
- StorageWorks Fibre Channel RAID Array 4100

You can use this software with these StorageWorks RAID Arrays configured to operate on Intel-based platforms running the Windows 2000 Advanced Server operating system in single-host server and Microsoft Cluster Service (MSCS) high-availability environments, in both standalone and clustered configurations.

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

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

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

Features

Secure Path provides the following features:

- Provides redundant physical connectivity management along independent Fibre Channel Arbitrated Loop (FC-AL) paths between switched dual-controller RAID systems and host servers equipped with multiple HBAs.
- Monitors each path and automatically re-routes I/O to a functioning alternate path if an HBA, cable, hub, switch or controller failure occurs.
- Determines the "health" of physical paths through the implementation of path verification diagnostics.
- Monitors and identifies failed paths and failed-over storage units.
- Facilitates online (static) load balancing between multiple storage systems.
- Automatically restores failed-over storage units to repaired paths with auto-failback capability enabled.
- Prevents failover/failback thrashing caused by marginal or intermittent conditions.
- Detects failures reliably without inducing false or unnecessary failovers.
- Implements failover/failback actions transparently without disrupting applications.
- Provides Client/Server remote management capability, and multiple storage system support.

Secure Path Technology

Key to Secure Path's functionality is the capability of StorageWorks RA4000/4100 array controllers to operate in an active/passive implementation, where one RA4000 Controller actively processes I/O, and an alternate controller remains passive.

Available storage units are preferred to the active controller. This determines which controller is used for access at system boot time. During runtime,

storage units may be moved between controller paths at any time through use of the Secure Path Management utility.

The Secure Path software detects the failure of I/O operations on a failed path and automatically re-routes traffic to an alternate path. Secure Path can detect and recover from controller, switch, hub, HBA or other connection failures. 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, 0+1, 1, 4, or 5. Secure Path will support either FAT or NTFS file system formats on single host configurations. Microsoft requires the NTFS file system in MSCS configurations.

Auto-Failback

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

Path Verification

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

Static Load Balancing

Secure Path takes advantage of the potential for multiple path access and enhances I/O performance through the use of online (static) load balancing. With this feature, Secure Path can be manually configured to distribute I/O operations across multiple storage systems.

Software Components

The Secure Path Software Kit includes the following software components:

- **RDFIL.sys** is a Windows filter driver that prevents the operating system from interpreting broken paths to LUNs as hardware removals. It disables unsafe removal of hardware by simply not acknowledging that the hardware is missing
- **RaiDisk.sys** is a Windows filter driver that provides the primary failover capability in the Secure Path product. RaiDisk supports StorageWorks RAID Array 4000/4100 multiple path access, and provides all functions required for monitoring I/O and detecting path failures.
- **Secure Path Manager** is the client/server application used to manage multiple path StorageWorks RAID Array 4000/4100 configurations. It displays a graphical representation of multiple path environments, indicating status of all configured storage units and paths. It runs locally at the managed servers, or remotely at a management workstation. The client is compatible with any of the Windows 2000 operating systems.

  To facilitate online (static) load balancing, Secure Path Manager provides the capability to move storagesets between paths. It indicates which path is currently servicing each configured storage unit, and displays the mode and state information for all available paths.
- **Secure Path Agent** is a Windows service that communicates with the RaiDisk filter driver on the host server, and Secure Path Manager on the client side, using the TCP/IP protocol and the WinSock API. It installs on the host server along with the RaiDisk driver.
- **Secure Path Setup** supports driver and application installation and de-installation with Windows 2000 Advanced Server operating system.

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

Chapter **2**

Technical Description

Overview

Compaq SANworks Secure Path for Windows 2000 on RAID Array 4000/4100 is a server-based software product that enhances these StorageWorks RAID Array storage systems by providing automatic recovery from server-to-storage system connection component failures. Secure Path supports multiple I/O paths between host and storage, improving overall data availability. If any component in the path between host and storage fails, Secure Path redirects pending and subsequent I/O requests to an alternate path.

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

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

Managed Entity Profiles

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

The profile limits for Secure Path Manager are a maximum of 2 servers (host systems) connected to and sharing up to 9 storage systems, configured for multiple-path failover mode. The host servers may be standalone servers or grouped into clusters. All servers in the profile must have access to all of the storage systems listed in that profile. Access to storagesets must be restricted to a single standalone server or a single "clustered" host set.

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

Controller Ownership

The RA4000/4100 storage system contains a pair of redundant controllers and supports the active/passive implementation, or operational model.

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

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

Path Definition

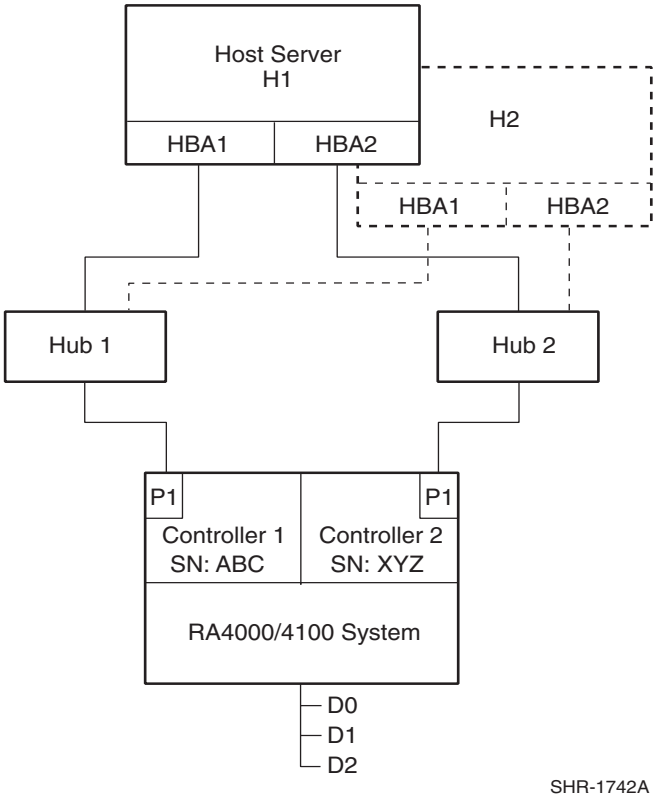
Within Secure Path, a path is defined as the collection of physical interconnect components including HBAs, switches or hubs, cables, and RA4000 Controllers. The Secure Path filter driver component, RaiDisk, distinguishes physical paths by elements of the SCSI equivalent address (Bus-Target-LUN) as derived by the HBA.

In FC-AL configurations, devices are accessed within Windows 2000 using conventional SCSI addressing terminology. Fibre Channel adapters are

referred to as HBAs, which are named and numbered as SCSI ports and/or physical locations. SCSI addresses are derived from the ALPA (Arbitrated Loop Physical Address), which is soft-assigned by the RA4000 Controller.

The LUN number is derived from the unit number assigned to the storageset within the controller using the Array Configuration Utility (ACU), included on the Compaq SmartStart CD. Each connected node on an arbitrated loop has a unique ALPA assignment.

In Figure 2-1, HBA 1, Hub 1 and Controller 1 - Port 1 constitute one arbitrated loop. HBA 2, Hub 2 and Controller 2 - Port 1 constitute another arbitrated loop.



	Host	Controller Serial No.	SCSI Port	Bus-Target-LUN	HBA Slot
Drive D: (D1)	H1	ABC	1	1 –1 –1	2
	H1	XYZ	2	1 –2 –1	3
	H2	ABC	1	2 –1 –1	2
	H2	XYZ	2	2 –2 –1	3

Figure 2-1. Path definition in an RA4000/4100 Secure Path FC-AL configuration

Path Status

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

Path Mode

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

- **Preferred Path Mode** indicates the user-specified path that will be used to communicate from a specific host to the specified storageset. RaiDisk declares the path to the owning controller as the Preferred path. The user may modify the default driver's path settings using Secure Path Manager.
- **Alternate Path Mode** indicates an alternate path. Alternate paths provide the redundancy in case preferred paths fail.
- **Offline Path Modes** (Preferred-Offline or Alternate-Offline) include the original mode (via the prefix) and indicate the user has specified the path should never be used for I/O. Paths are marked offline only as a result of user intervention.

NOTE: Offline Mode can not be applied to paths that are in an Active State.

Path State

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

- **Active State** indicates the associated path is currently servicing, or is capable of servicing, I/O to the storageset.
- **Available State** indicates the associated path belongs to the set of redundant paths to the storageset that could be utilized during failover.
- **Failed State** indicates the path has encountered errors either during normal operation or as a result of Path Verification testing.

Chapter 4, "Managing Secure Path," provides a more detailed discussion of Path Modes and Path States, and provides illustrative examples of the effects of failover, failback, and user intervention.

Failover Operation

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

Secure Path does not change the mode of "Preferred" or "Alternate" paths in failover situations, so you can restore original path assignments after making repairs. Secure Path marks the "Preferred-Active" path failed and switches to an "Alternate – Available" path.

Secure Path attempts to move the device to an "Alternate – Available " path on the other controller. Secure Path changes the "Alternate-Available" path to "Alternate-Active."

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

Failback Options

Secure Path allows manual or automatic path failback.

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

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

Path Verification

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

Path Verification is useful for detecting failures that affect overall path redundancy before they affect failover capability. If a "Preferred" path fails

path verification, failover occurs. If an "Alternate" path fails path verification, its state will change from "Available" to "Failed."

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

Anti-thrash Filter

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

In order to utilize anti-thrash filtering, Path Verification, which is enabled by default, must be disabled.

Path Management Behavior Summary

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

Table 2-1
Path Management Behavior Summary

Startup	1) Choose path to controller on which LUN is online as **preferred active** –path to other controller is marked **alternate available**. 2) If no online path is found, make an available path online and use as **preferred active** – other path marked **alternate available.**
Active Path Failure	1) Path marked **preferred (or alternate) failed** and fails to **alternate available** path. **Alternate available** path used is marked **alternate active**. 2) Behavior is the same with I/O or background path verification. 3) If LUN reserved, mark 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 auto-failback 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.

Chapter **3**

Installing Secure Path

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

- Reference material for high-availability connection options
- Installation prerequisites
- Installation procedures for Secure Path Fibre Channel standalone and cluster configurations
  - Server software installation – RDFIL and RaiDisk filter drivers, and Secure Path Agent
  - Client software installation - Secure Path Manager GUI

Components Required for RA4000/4100 Fibre Channel Secure Path Installation

Verify receipt of the Secure Path software kit and the Fibre Channel hardware ordered for the installation. If you are missing any component, please contact your account representative, or call the Compaq Customer Services Hotline at (800) 354-9000.

The basic requirements for Secure Path operation are listed in Table 3–1.

Table 3-1
Secure Path Fibre Channel Installation Prerequisites

Host Feature	Requirement
Platform	ProLiant and other x86
Operating System	Windows 2000 Advanced Server Edition, Service Pack 1
Secure Path Software Kit	SANworks Secure Path for Windows 2000 on RAID Array 4000/4100 Version 3.1
RAID Storage System(s)	StorageWorks RAID Array 4000 StorageWorks RAID Array 4100 RA4100 Controller Firmware Version 2.58
Solution Software Kit	Compaq SmartStart and Support Software 4.90 Compaq Management Software 4.90
Cluster Kit (optional)	Compaq ProLiant Cluster HA/F200 Kit (for Cluster services)
Host Bus Adapter(s) (and adapter driver)	Supported models for Windows 2000 –Intel and RA4000/4100: StorageWorks 64-Bit/66-MHz Fibre Channel Host Adapter StorageWorks Fibre Channel Host Adapter/P
Fibre Channel Interconnect Hardware	FC-AL hubs, switches, and connection hardware as required
Service Tools	Appropriate tools to service the equipment
Technical Documentation	The reference guides for the RAID system, HBA, host server and Windows software

Installing an RA4000/4100 Secure Path Configuration

This section provides procedures to install and configure a Secure Path topology for Fibre Channel hardware installation.

Hardware and Standalone Software Setup

To install and configure a Secure Path Fibre Channel topology for standalone (non-clustered) systems:

1. Install all Windows servers and all HBAs, referencing the user documentation included with your hardware. Do not connect HBAs to hubs or switches at this time.
2. Install Windows 2000 Advanced Server using SmartStart 4.90 assisted installation utility.
3. Install Secure Path software on the Windows server(s).

   The Secure Path software is installed using the Secure Path setup wizard. Please refer to the "Secure Path Software Installation" section below to complete the Secure Path software installation setup.
4. Shut down the server.
5. Install all of the new RAID storage system and FC-AL interconnect hardware (hubs/switches) and cabling according to the instructions provided with the installation documentation shipped with the Fibre Channel equipment.
6. Restart the server.

   Create storagesets and provide unit attributes for LUNs using the Array Configuration Utility (ACU) included with SmartStart 4.90.
7. Enter the Windows 2000 Disk Manager to configure basic disk storage.
8. Restart the server.

   Following system reboot, verify the Windows system Event Log shows a successful RaiDisk driver start event.

   Verify the Windows application Event Log shows a successful Secure Path Agent start event.

Hardware and Cluster Software Setup

Refer to the *Compaq ProLiant Cluster HA/F200 Configuration Poster*, included with your Compaq ProLiant Cluster HA/F200 Kit, for hardware and cluster software setup and configuration.

Secure Path Software Installation

Server Software Installation

Install Secure Path Server software on the Windows host system to which the RAID storage system is connected. TCP/IP installation is a requirement for the host system. For cluster configurations, Secure Path must be installed on each member of the cluster.

IMPORTANT: The installation of Secure Path requires that a Temp directory be available on the system drive. For example: C:\Temp

---

Install the Secure Path Server software as follows:

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

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

   where: *drive_letter* is the drive letter assigned to the CD-ROM
3. When the setup starts, choose the destination path. Then choose the "Secure Path Server Install" option to install the required drivers and Agent on your server.

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

   Check with your system administrator to assure proper TCP/IP network configurations and protocols.
4. Enter a validation password. For cluster configurations, make sure the password is the same for each member of the cluster.

Client Software Installation

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

Install the Secure Path Client software as follows:

1. Insert the *Compaq SANworks Secure Path Software* CD into your CD-ROM drive.
2. If you have AutoRun enabled, the Secure Path setup program will start automatically. Otherwise, Choose "Run" from the START menu and enter the following command:

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

   where: *drive_letter* is the drive letter assigned to the CD-ROM
3. When the setup starts, choose the destination folder. Then choose the "Secure Path Client Install" option to install the Secure Path Manager software.

You have now completed the software installation procedures required to support the Secure Path environment. See Chapter 4, "Managing Secure Path," for information on monitoring and managing Secure Path activity using Secure Path Manager.

Chapter 4

Managing Secure Path

This chapter provides the following Secure Path Manager operational information:

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

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

Launching Secure Path Manager

To launch SPM:

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

Logging on to Secure Path Manager

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

Defining SPM Storage Profiles

SPM displays a *storage-centric* view of Secure Path managed RAID storage resources. All Secure Path protected RA4000/4100 storage systems common to a given host (or set of hosts) are presented in an SPM display.

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

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

A single instance of SPM is capable of managing:

- Two non-clustered hosts sharing one or more RA4000/4100 storage systems
- One set of clustered-hosts sharing one or more RA4000/4100 storage systems

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

Figure 4-1 shows an example of an SPM login display.

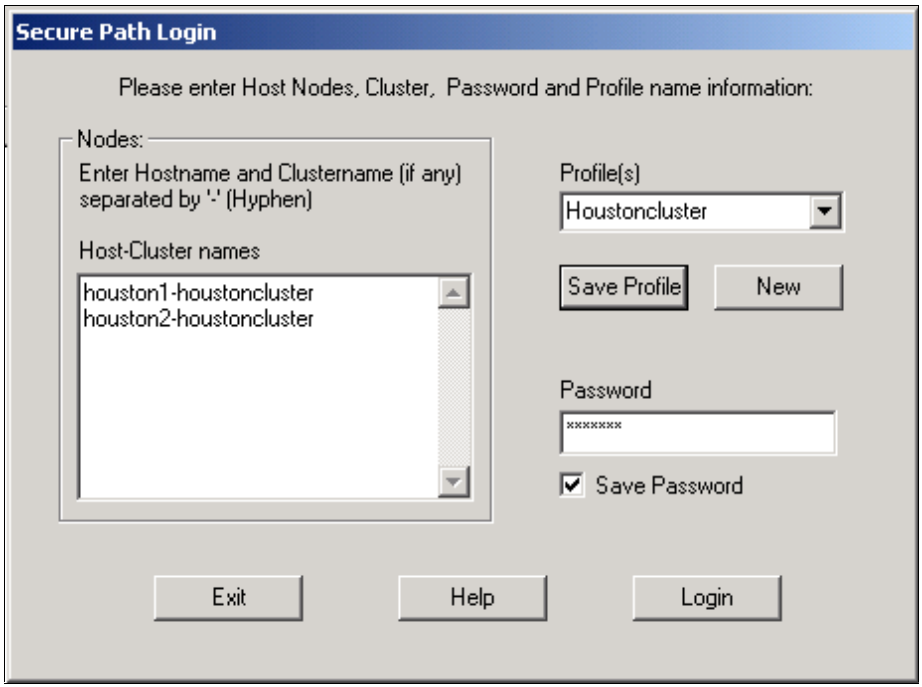


Figure 4-1. SPM login window with a clustered host storage profile

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

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

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

Saving an SPM Storage Profile

To save an SPM profile:

1. Enter a unique name in the "Profile(s)" field once you have defined a storage profile.
2. Save the profile by clicking "Save Profile."

Creating A New SPM Storage Profile

To create additional SPM storage profiles:

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

Selecting an Existing SPM Storage Profile

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

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

Editing an Existing SPM Storage Profile

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

Changing the Secure Path Agent Password

To change the Secure Path Agent's password:

1. Run the Secure Path Agent Configuration utility located in the Secure Path program folder from the Start Menu.
2. Once you have changed the Agent's client (SPM) access list or password using the Configuration utility, you must stop and restart the Agent using the Administrative Tool Services located in Control Panel.

3. Find and select the Secure Path Agent in the list of services and click "Stop."
4. Once the Agent has stopped, select Secure Path Agent again and click "Start."

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

Troubleshooting Connection Problems

If you experience problems attempting to log on to SPM, see Chapter 5, "Troubleshooting Secure Path Connection Problems," for more information.

Monitoring Host Connections

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

NOTE: If you have problems authorizing client connections using Fully Qualified Domain Names (FQDN), it may be due to a Domain Name Service (DNS) resolution issue, and can be resolved by a *HOSTS* file entry containing relevant FQDN to IP address mapping.

As shown in Figure 4-2, a server icon is displayed for each host in the window frame located immediately below the tool bar. The host's name is listed above the icon and a cluster name is listed below if it is a member of a cluster.

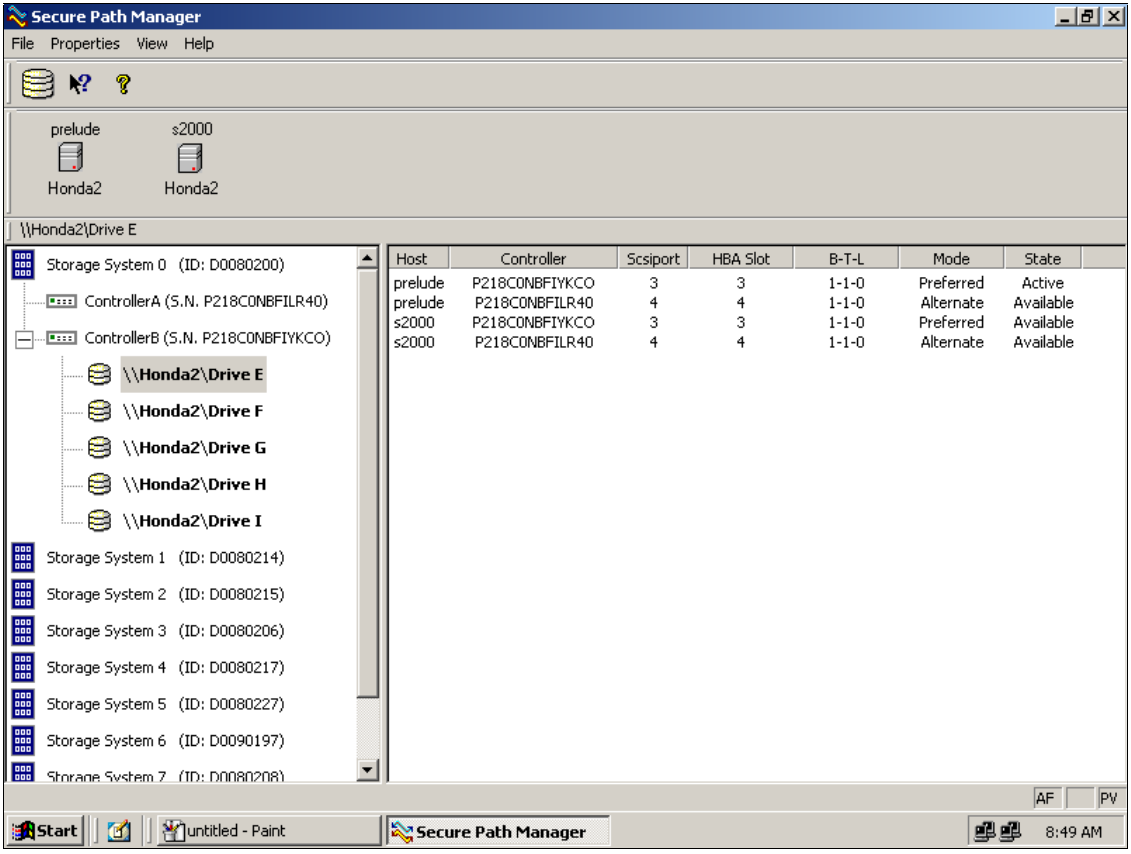


Figure 4-2. Host connection monitor

SPM monitors its connection with each member of a storage profile and will indicate a loss of connection to a particular host with a red “X.” Figure 4-3 shows SPM has lost connection to the “Honda2” cluster member “prelude.”

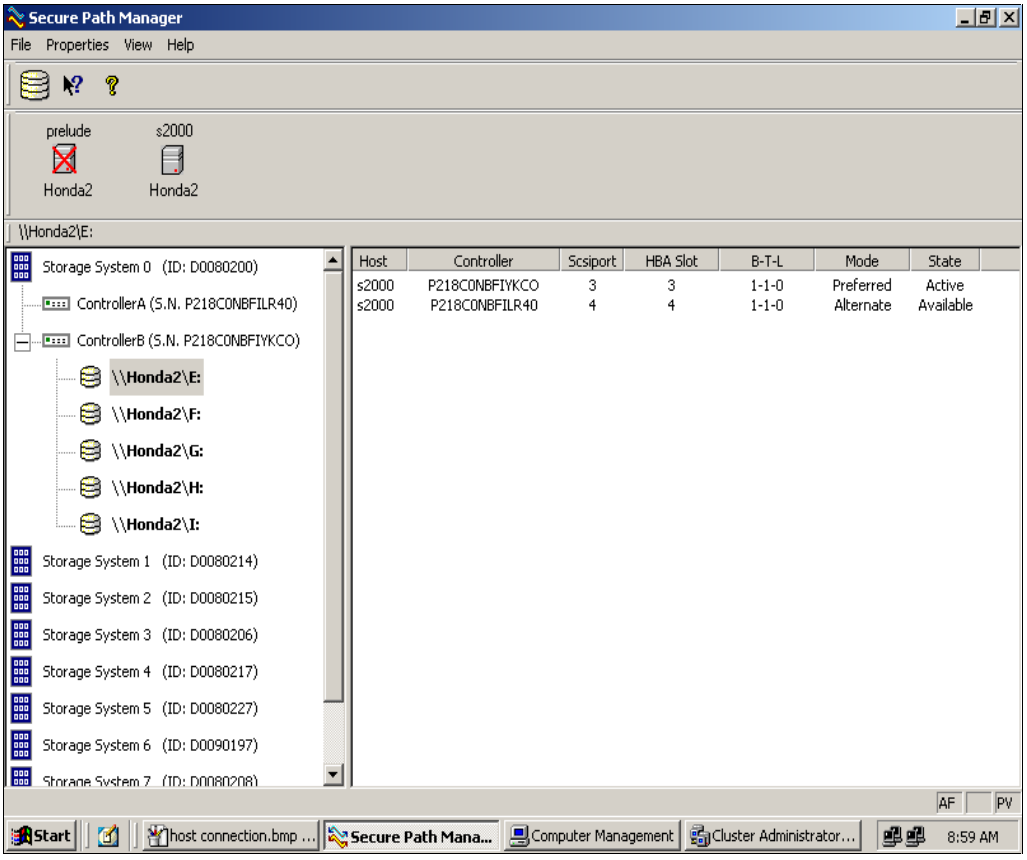


Figure 4-3. Lost host connection Icon

Responding To A Lost Host Connection

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

- A loss of connection does not necessarily mean that you have lost Secure Path's protection capability for storage on that host. If the host is still running, the problem is most likely due to a network connectivity problem and you have only lost Secure Path remote management functions. Secure Path's RaiDisk multiple path driver is still protecting availability to your storage.
- If the host is a member of a cluster, SPM will continue to report storage information based on data received from the surviving host or hosts.
- If the host is a member of a cluster, check your cluster management utilities to determine whether storage resources have failed-over to a surviving host.
- If the host is still running or following a reboot, run Windows Event Viewer and examine the Application and System logs to determine what happened prior to and during the loss of connection. In particular, check for network issues that may have caused a connectivity problem between the host and the SPM client.
- SPM will automatically re-establish communication to a host when the connection becomes available.

Setting Storage Profile Properties

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

- Enable or Disable the **Auto-Failback** policy (default = *disabled*). When Auto-Failback is enabled, all storagesets that have failed-over to an alternate path will automatically failback to their Preferred path when access to that path is restored. Storagesets will failback automatically only if I/O operations to those storagesets are in process. Auto-failback enabled in conjunction with Path Verification enabled permits failback to occur for quiescent storagesets.

- Enable or Disable **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 effect on the current configuration. The Polling Interval is user selectable from a minimum 5 seconds to a maximum of 30 minutes.

Storage System View

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

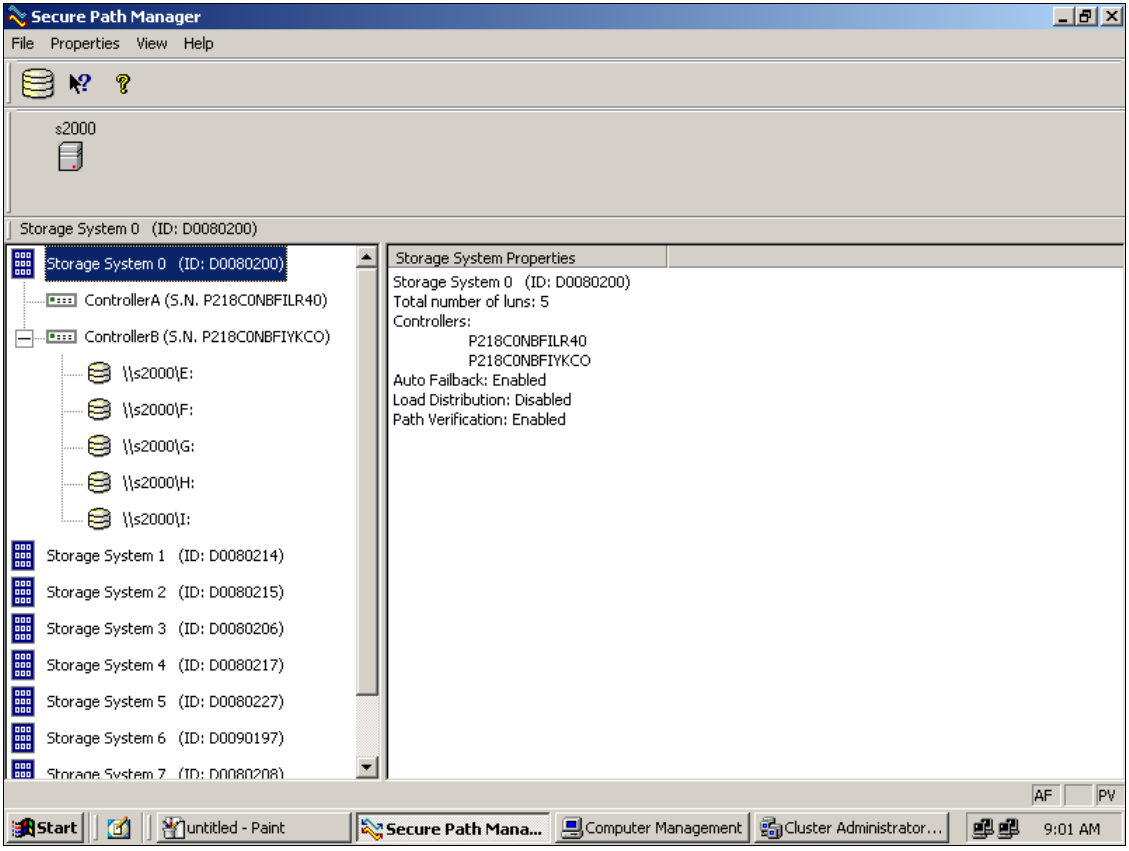


Figure 4-4. SPM single host storage profile –Storage System view

Storage Systems and Controllers

- **Storage System ID** - Each RA4000/4100 storage system is identified by a unique 64-bit value.

  For RA4000/4100 storage systems, the Storage System ID is determined at time of manufacture and stored in controller NVRAM. The Storage System ID remains constant for the life of the RAID storage system.

- **Controller Serial Number** - The individual controllers of an RA4000/4100 storage system are identified by a unique 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 Disk Manager.
- **Drive Letter** – the logical drive letter assigned by the Windows Disk Manager.
- **Bus/Target/LUN** – the physical address representing the connection to the host server.
- **Volume Label** – the label assigned to the volume by the user with Windows Explorer or Disk Manager.

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.

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.
- **Scsiport** – represents the physical port number of the Host Bus Adapter servicing the path. The HBA is a relative number determined by the Windows "order of discovery" for adapters on that host.
- **HBA Slot** – identifies the host node PCI slot containing the identified HBA.
- **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 4-5) shows a single-host configuration with the host "s2000" attached to multiple Secure Path protected RAID storage systems.

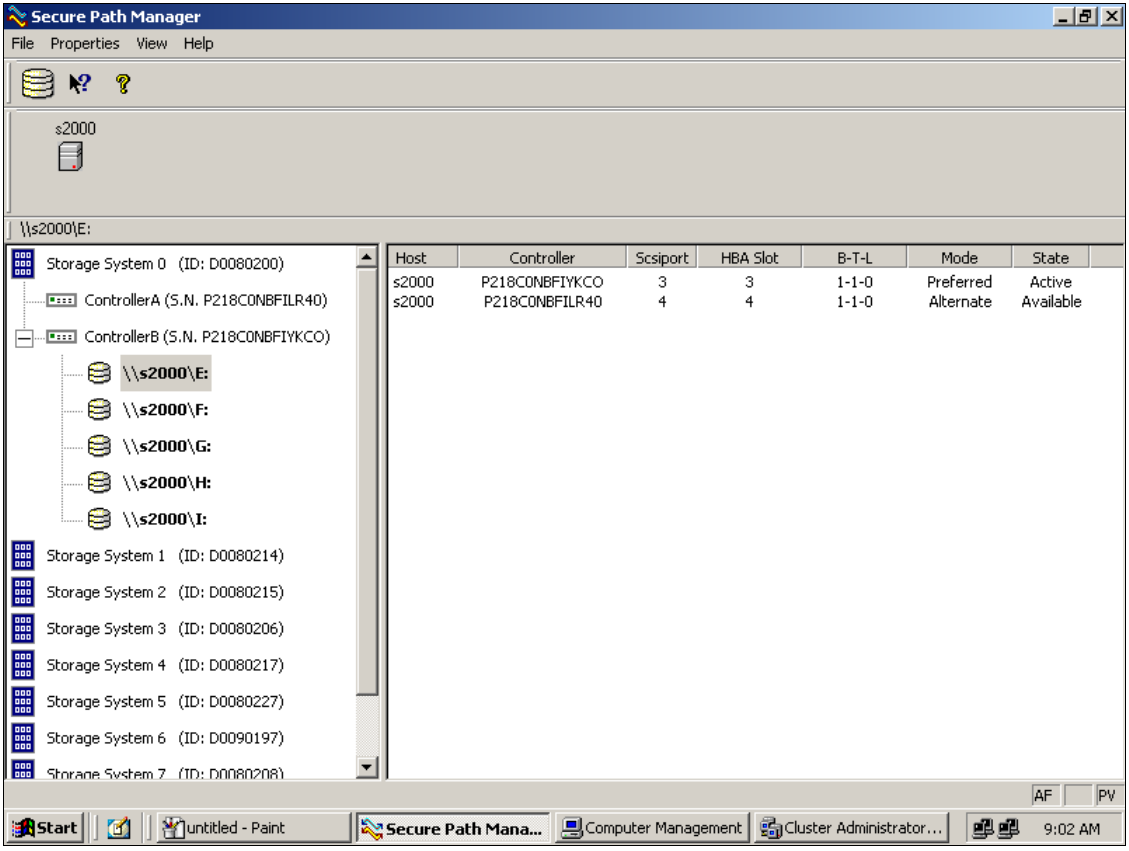


Figure 4-5. SPM single host, multi-array storage profile – Physical Path view

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

The display information in this example shows two paths configured from host "s2000" to drive E. Both of the paths access the storageset at Bus 1, Target 1, and LUN 0 through the HBA at Ports 3 and 4, respectively, with one path Preferred and the other path Alternate.

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

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

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

The path in the Available State has a different serial number than that of the Preferred Mode path, indicating that it is providing standby access through the other controller. If the controller currently servicing the Preferred path fails, the path on the surviving controller transitions to the Preferred State.

Polling Interval and Display Refresh

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

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

Managing Storagesets and Paths

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

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

The following SPM actions are built into the SPM GUI, but will appear grayed-out, as they are not applicable to RA4000/4100 storage systems.

- Make a path Alternate
- Make a path Preferred
- Change the Preferred path
- Load Distribution

Moving A Storageset

Choose "Move a Storageset" when you want to change the ownership from the current RA4000 Controller to the other. This action is useful if you need to manually return a failed-over storageset to its Preferred path when Auto-Failback has been disabled.

There are two methods available to move a storageset.

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

All LUNs on the specified RA4000/4100 storage systems move together, as a group, between controllers.

Making A Path Offline

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

1. Click an Alternate Available or Preferred Available path. A path in Active State cannot be changed to Offline mode.
2. Right click to select the “Make Offline” action.

If the path was Alternate Available, its mode will change to alt-offline. If the path was Preferred Available, 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 Offline mode to its original Online mode. To make a path online:

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

If the path was alt-offline, its mode will change to Alternate Available. If the path was pre-offline, its mode will change to Preferred Available.

Verifying A Path

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

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

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

Repairing A Path

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

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

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

Detecting and Identifying Path and Controller Failures

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

In addition, failover events are logged by the RaiDisk driver in the Windows Event Viewer.

You should routinely monitor SPM status to check for occurrences of failover events that might compromise either the performance or availability of storage resources.

Availability is compromised if your configuration includes only two configured paths to a storageset and one is lost due to component failure. Secure Path will be unable to failover to a redundant path should a subsequent fault occur in this situation.

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

Detecting Path Failures

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

Storage System Path Failure Detected

The icon shown in Figure 4-6 indicates that a failure of at least one, but not all paths to that RA4000/4100 storage system was detected by Secure Path. Browse the storage system to determine the affected controller and storagesets.

Figure 4-6. Storage system path failure detected

Storage Controller Path Failure Detected

The icon shown in Figure 4-7 indicates that a failure of at least one, but not all paths to that storage controller was detected by Secure Path. Browse the storage controller to determine the affected storageset(s).

Figure 4-7. Controller path failure detected

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

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

Storageset Path Failure Detected

The icon shown in Figure 4-8 indicates that a failure of at least one, but not all paths to that storageset was detected by Secure Path. Click on the storageset to highlight it and examine the Physical Path view information to determine the specific nature of the path failure.

Figure 4-8. Storageset path failure detected

Total Path Failures

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

Figure 4-9. Storage system failure detected

Figure 4-10. Storage controller failure detected

Figure 4-11. Storageset failure detected

Identifying Path Failovers

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

- Was I/O active on the affected storageset?

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

- Is Path Verification enabled?

  Path Verification periodically tests the viability of all paths and will automatically detect faults on the Preferred and Alternate path. This means that a controller failover will result in a FAILED state for the Preferred path.

Identifying Controller Failovers

An RA4000 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 4-10. SPM will show that all storagesets previously on this controller have been failed-over to the surviving controller. Because all of the Alternate paths to the faulty controller have transitioned to the FAILED State because of Path Verification, storageset path failure icons will be displayed for each storageset on the surviving controller.

Responding to Failover Events

When investigating possible problems with failovers, consider the following:

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

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

Using SPM with MSCS Clusters

In Microsoft Cluster Service (MSCS) environments, the SPM display will always show the associated cluster name alongside the storageset in the Storage System view. When you highlight a storageset, SPM will display all of the physical paths from each cluster host to that particular storageset in the Physical Path view.

MSCS 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.

Chapter 5

Troubleshooting Secure Path Connection Problems

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

- Client/Agent considerations
- Network considerations

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

Client/Agent Considerations

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

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

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

Network Considerations

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

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

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

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

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

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

- Client names that exceed 15 letters or carry a dot require an entry for that name in the *HOSTS* file or resolution by a DNS server. It is also possible to have DNS resolve NetBIOS names as long as the DNS server is updated with the appropriate information.

- 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 (FQDN) with DNS.

- For production environments, where management and security are a concern, it is recommended that fully qualified names be used with DNS name resolution.

- For test and evaluation environments it is usually easier to simply add the server's name to the client's *HOSTS* file and the client's name to the server's *HOSTS* file.

- Make sure that you can "ping" the Secure Path host, both locally and from a remote host using the host name, not the IP address.

Appendix A

Glossary

Bus For Fibre Channel configurations, HBAs may use multiple bus numbers as an artificial method of expanding bus address space.

Controller A controller is a hardware device that facilitates communication between a host and one or more LUNs organized as an array. The RA4000 Controller is an array controller supported for use with Secure Path. Each controller in an RA4000/4100 storage 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-path mode by a unique 64-bit identifier that is displayed next to the subsystem icon.

HBA An HBA (Host Bus Adapter) is an I/O device which serves as the interface connecting a host system to the SCSI bus or Fibre Channel Arbitrated Loop. HBAs are assigned a relative port number by the Windows operating system according to order of discovery (see Port).

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

LUN A LUN (Logical Unit Number) is the actual unit number assigned to a device at the RAID system controller.

Mode Mode is a user-selectable parameter that specifies path behavior during nominal and failure conditions. Paths may be set to one of the following modes:

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

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

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

State State is an attribute that describes the current operational condition of a path. A path may exist in the following state(s):

- **Active** - indicates a path that is currently servicing I/O requests.
- **Failed** - indicates a path that is disabled and not actively servicing I/O requests.
- **Available** - indicates a path that is neither Active nor Failed.

Target The target number is assigned by a mapping function at controller level and is derived from ALPA (Arbitrated Loop Physical Addresses) in an FC-AL topology.

Appendix ***B***

Removing Secure Path Software

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

To remove Secure Path software from your system:

1. Launch Control Panel and choose “Add/Remove Programs.”
2. Select “SANworks Remove Secure Path Client.”
3. Click OK in the resulting window.
4. Select “Remove SANworks Secure Path Server.”
5. Click OK in the resulting window.
6. Shut down the system.
7. Remove redundant paths from the controller pairs.

The Secure Path software removal process is complete.

NOTE: To aid in the reinstallation of Secure Path, the file ‘client.ini, is not removed.

Index

T

U

W