installation guide

hp StorageWorks secure path V3.1c for Windows on raid array 4000/4100

Product Version: 3.1C

Third Edition (September 2003)

Part Number: AA–RN0DC–TE

This installation guide provides procedures for setting up, configuring, and managing Secure Path V3.1C for Windows on RAID Array 4000/4100 on Windows Server 2003.

Printed in the U.S.A.

Secure Path V3.1C for Windows on Raid Array 4000/4100 Installation Guide
Third Edition (September 2003)
Part Number: AA–RN0DC–TE

contents

Figures

Tables

about this guide

This HP StorageWorks Secure Path Version 3.1C for Windows on RAID Array 4000/4100 (Secure Path) installation guide provides information to help you:

- Plan, install, and configure HP StorageWorks RAID Array 4000/4100 hardware
- Install Secure Path software
- Contact technical support for additional assistance

About this Guide topics include:

Overview

This section covers the following topics:

Intended Audience

This guide is intended for use by system administrators who are experienced with the following:

- Microsoft Windows 2003
- HP StorageWorks Fibre Channel RAID Array 4000
- HP StorageWorks Fibre Channel RAID Array 4100

Related Documentation

In addition to this guide, HP provides the *HP StorageWorks Secure Path Version 3.1C for Windows on RAID Array 4000/4100 Release Notes*.

Conventions

Conventions consist of the following:

- Document Conventions
- Text Symbols
- Getting Help

Document Conventions

The document conventions included in Table 1 apply in most cases.

Table 1: Document Conventions

Element	Convention
Cross-reference links	Blue text: Figure 1
Key and field names, menu items, buttons, and dialog box titles	**Bold**
File names, application names, and text emphasis	*Italics*
User input, command and directory names, and system responses (output and messages)	`Monospace font` `COMMAND NAMES` are uppercase monospace font unless they are case sensitive
Variables	*`<monospace, italic font>`*
Website addresses	Blue, underlined sans serif font text: http://www.hp.com

Text Symbols

The following 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 death.

Caution: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or data.

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

Getting Help

If you still have a question after reading this guide, contact an HP authorized service provider or access our website: http://www.hp.com.

HP Technical Support

In North America, call technical support at 1-800-652-6672, available 24 hours a day, 7 days a week.

Note: For continuous quality improvement, calls may be recorded or monitored.

Outside North America, call technical support at the nearest location. Telephone numbers for worldwide technical support are listed on the HP website under support: http://www.hp.com/country/us/eng/support.html.

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

HP Storage Website

The HP website has the latest information on this product, as well as the latest drivers. Access storage at:
http://www.hp.com/country/us/eng/prodserv/storage.html.

From this website, select the appropriate product or solution.

HP Authorized Reseller

For the name of your nearest HP authorized reseller:

- In the United States, call 1-800-345-1518
- In Canada, call 1-800-263-5868
- Elsewhere, see the HP website for locations and telephone numbers: http://www.hp.com.

Installation Prerequisites

1

This chapter describes prerequisite information for installing Secure Path V3.1C for Windows on RAID Array 4000/4100 for use with the following storage systems:

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

Note: Make sure you complete the tasks in the installation check list before proceeding with the installation.

Secure Path Prerequisites

Table 2 lists the system prerequisites for Secure Path V3.0C installation.

Table 2: Secure Path Installation Prerequisites

Host Feature	Requirement
Operating Systems	Windows Server 2003
Secure Path Software Kit	Secure Path V3.1C for Windows on RAID Array 4000/4100
RAID Storage Systems	StorageWorks RAID Array 4000 StorageWorks RAID Array 4100 RA4100 Controller Firmware Version 2.60
Solution Software Kit	HP SmartStart and Support Software 6.30 HP Management Software 6.30
Host Bus Adapter	HP StorageWorks 64-bit 66 MHz PCI-to Fibre Channel Host Bus Adapter (Part Number176479-B21)
FC Interconnect Hardware	Cables, switches and connection hardware as required (Application Notes provide detailed equipment part numbers).
Service Tools	Appropriate tools to service the equipment.

Installation and Configuration Information

Installation and Configuration Documentation

Before installing or updating Secure Path, be sure to review the installation and configuration information for your system. The HP website has the latest information at:

http://www.hp.com/country/us/eng/prodserv/storage.html.

Supported SAN Topologies

Secure Path for Windows supports SAN topologies as defined and described in the *HP StorageWorks SAN Design Reference Guide*, and other SAN technical documentation. This document is available on the HP website at:

http://h18006.www1.hp.com/products/storageworks/san/documentation.html.

Choose **SAN Design Reference guide**.

Installation and Configuration Checklist

Make sure you've completed the following tasks before installing Secure Path:

Table 3: Installation and Configuration Checklist

Task	
Obtain and review the latest documentation, including release notes, as described in Installation and Configuration Documentation on page 15.	☐
Verify receipt of the Secure Path software kit and the Fibre Channel hardware ordered for the installation. If you are missing any component, contact your account representative, or call the HP Customer Service Hotline at (800) 354-9000.	☐
Install all the hardware components as described in the hardware installation and configuration documentation.	☐
Make sure you have the updated drivers for the HBA, if necessary.	☐
Backup your computer.	☐

Installing Secure Path

2

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

Installing an RA4000/4100 Secure Path Configuration

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

Hardware and Standalone Software Setup

To install and configure a Secure Path 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 Server 2003 using SmartStart 6.30 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 Secure Path Software Installation on page 19 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 6.30.
7. Enter the Disk Manager and configure basic disk storage.
8. Restart the server.
9. Following system reboot, verify the Windows system Event Log shows a successful RaiDisk driver start event.
10. Verify the Windows application Event Log shows a successful Secure Path Agent start event.

Hardware and Cluster Software Setup

Refer to the HP ProLiant Cluster HA/F200 Configuration Poster, included with your HP 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.

Note: 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:

To install the Secure Path server software:

1. Access the CD:
   - If you have AutoRun enabled on your server, the Secure Path setup program starts automatically. Otherwise, Choose **Start > Run**, then browse to the *Launch.exe* program on the CD-ROM drive.
   - If you are accessing the CD on a Network drive, choose **Start > Run**, then browse to the *Launch.exe* program on the network drive.
2. Click **Yes** to agree to license terms.
3. Read the additional information and click **Next**.
4. Click **Next** to start the installation.
5. When the setup starts, choose the destination path. Then choose **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 includes the local host names for each cluster member.

   Check with your system administrator to assure proper TCP/IP network configurations and protocols.
6. 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 Secure Path Software CD into your CD-ROM drive.
2. If you have AutoRun enabled, the Secure Path setup program starts automatically. Otherwise, Choose **Start > Run** and enter the following command:

   drive_letter:\spinstal\setup.exe

   drive_letter is the drive letter assigned to the CD-ROM
3. Click **Yes** to agree to the licensing terms.
4. Click **Yes** to start the installation.
5. Read the additional information and click **Next**.
6. Click **Next** to start the installation.
7. Indicate whether you want to use an existing configuration file:
   a. Choose **Yes** to use existing configuration files. If you choose **Yes**, indicate which clients you want to use and click **OK**. The system completes the installation using existing configuration information. Go to step 8.
   b. Choose **No** to create a configuration file.
8. Click **Password**.

   Enter and confirm your new password.

Note: For cluster configurations, make sure the password is the same for each member of the cluster.

---

9. Click **Add Client**.
10. Enter the name of the client in the Client field.
11. Click **OK**.
12. Click **Exit**.
13. Click **Next** and do not review the log file.

14. Click **Finish** to complete your Secure Path software installation.

    You have now completed the software installation procedures required to support the Secure Path environment. See Chapter 3, page 23 for information on monitoring and managing Secure Path activity using Secure Path Manager.

Removing Secure Path Software

Use the following procedure 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. Choose **Control Panel > Add/Remove Programs.**
2. Choose **Remove Secure Path Client**, and click **OK**.
3. Choose **Remove Secure Path Server**, and click **OK**.
4. Shut down the system.
5. 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 *client.ini* file is not removed.

Managing Secure Path

3

This chapter provides the following Secure Path Manager operational information:

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 Secure Path, 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 1 shows an example of an SPM login display.

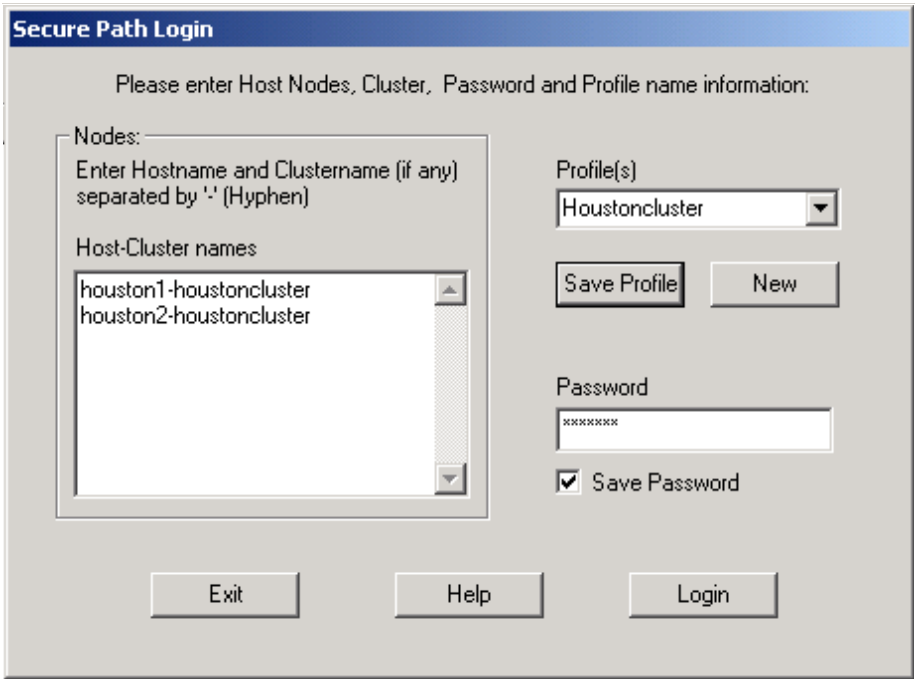

Figure 1: SPM login window with a clustered host storage profile

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).

Choose **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 **Profiles** 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 **Profiles** field.
4. Click **Save Profiles**

Selecting an Existing SPM Storage Profile

To choose an existing SPM storage profile, use the pull down arrow on the **Profiles** 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**. Once the Agent has stopped, select Secure Path Agent again and click **Start**.

The Agent restarts and updates its client and/or password database. Make sure that you do this for each of the hosts in an SPM storage profile. Refer to Troubleshooting Secure Path Manager Connection Problems on page 49 for information about network connection problems.

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 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.

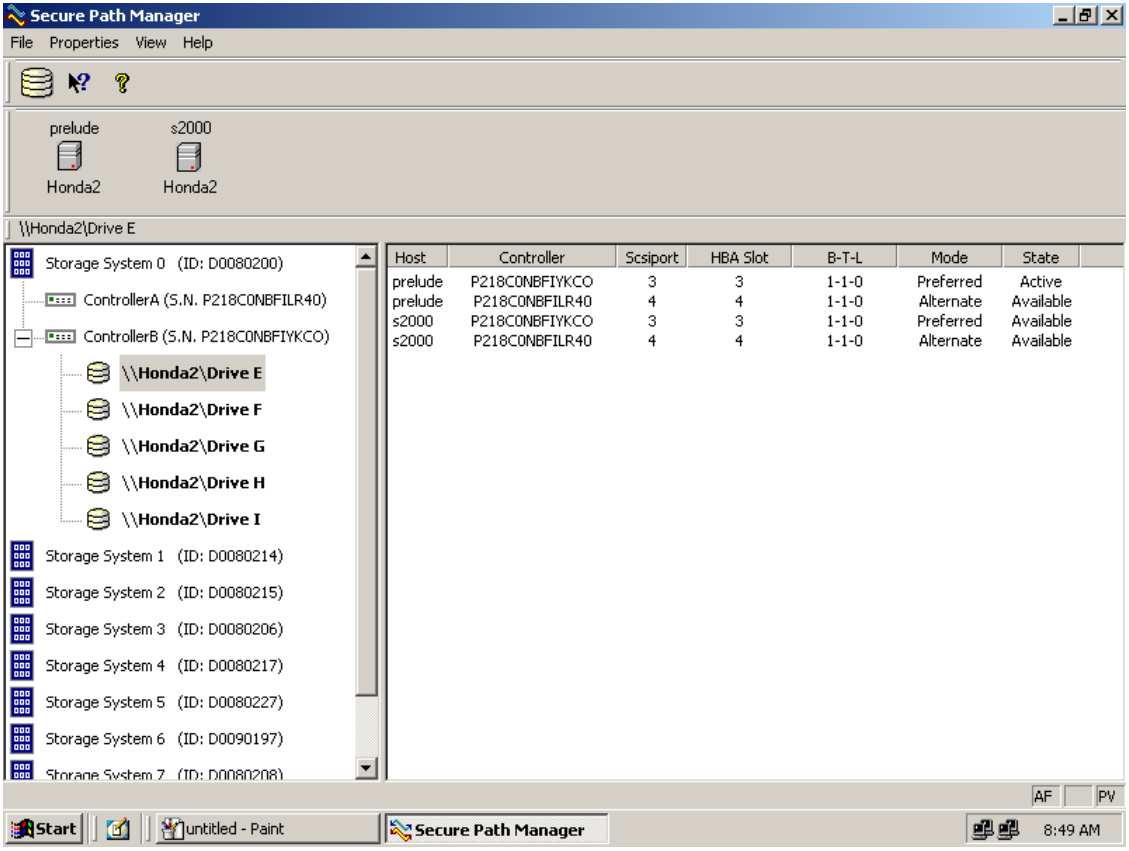

Figure 2: Host connection monitor

SPM monitors its connection with each member of a storage profile and indicates a loss of connection to a particular host with a red **X**. Figure 3 shows SPM has lost connection to the Honda2 cluster member prelude.

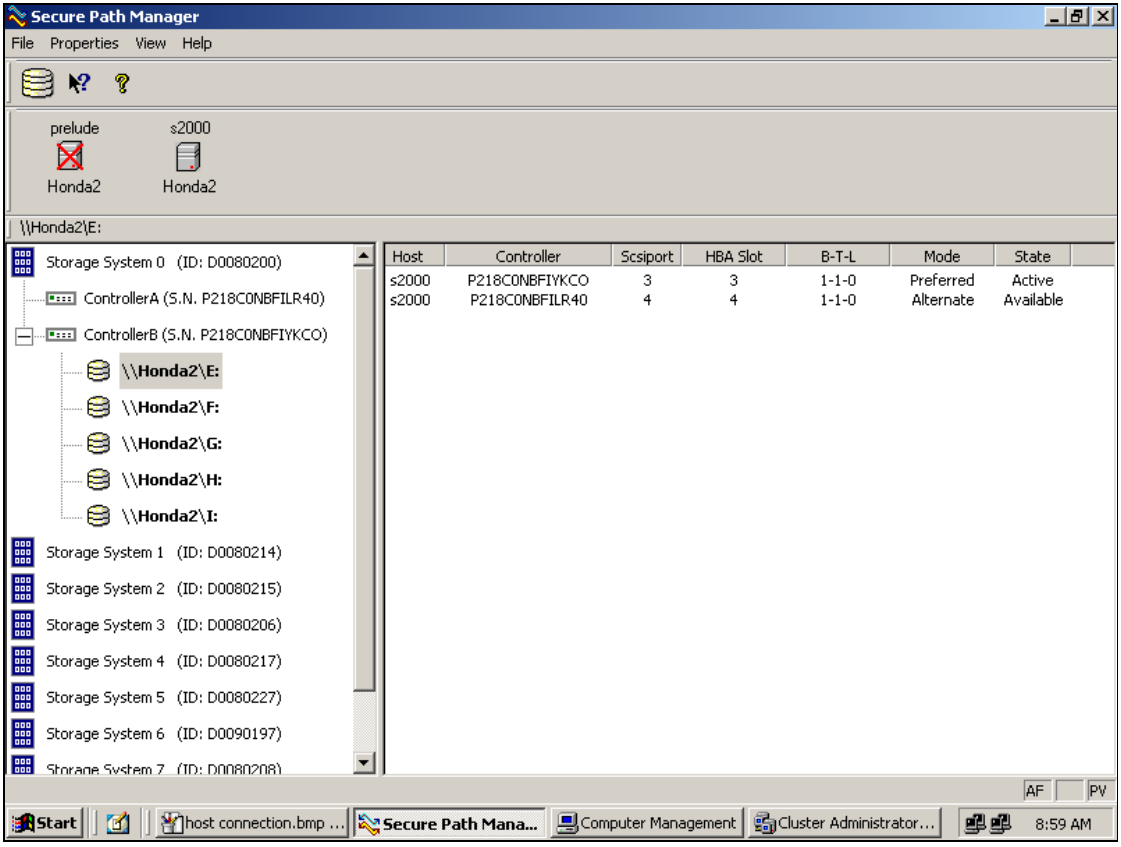

Figure 3: Lost host connection Icon

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 continues 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 automatically re-establishes 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 automatically fails back to their Preferred path when access to that path is restored. Storagesets fails back 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 requests 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 as shown in Figure 4. Browsing this view displays each of the RAID storage systems, controllers, and associated storagesets that comprise your Secure Path storage profile.

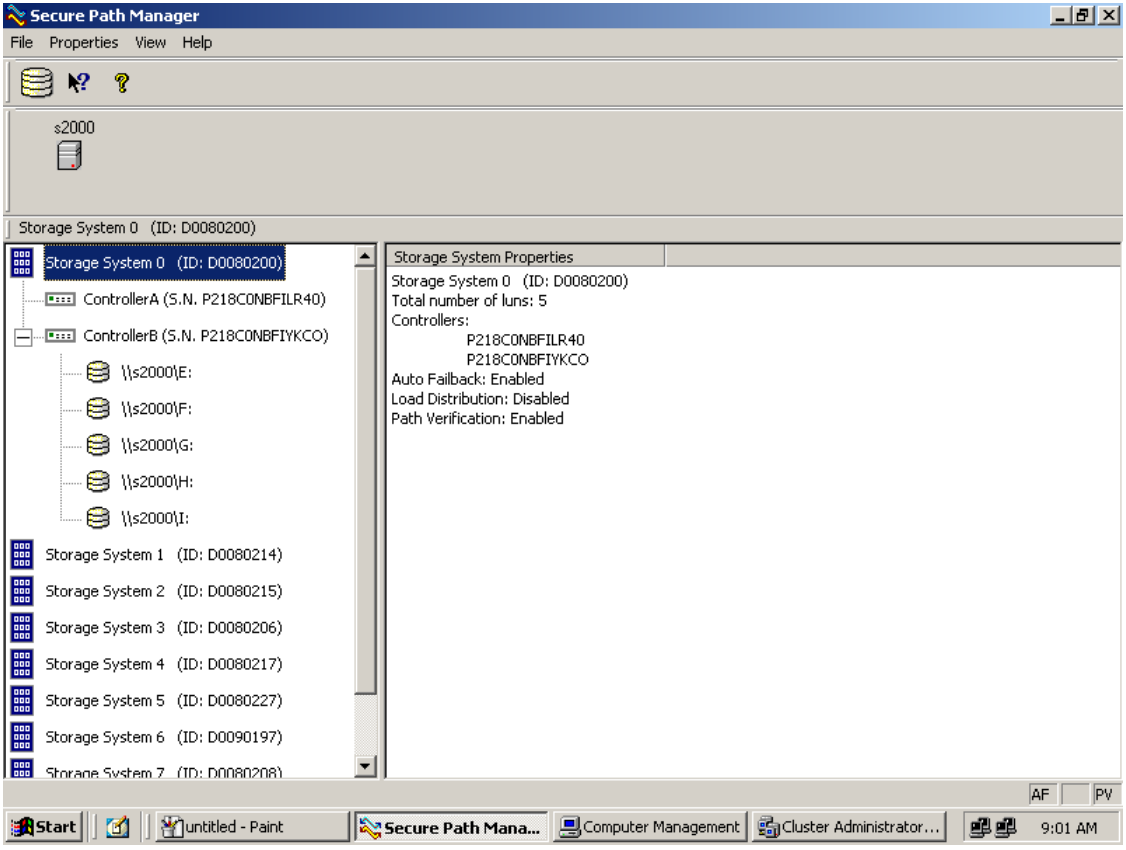

Figure 4: SPM Single Host Storage Profile – Storage System View

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 always displays 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.

In Figure 5, the SPM screen shows a single-host configuration with the host s2000 attached to multiple Secure Path protected RAID storage systems.

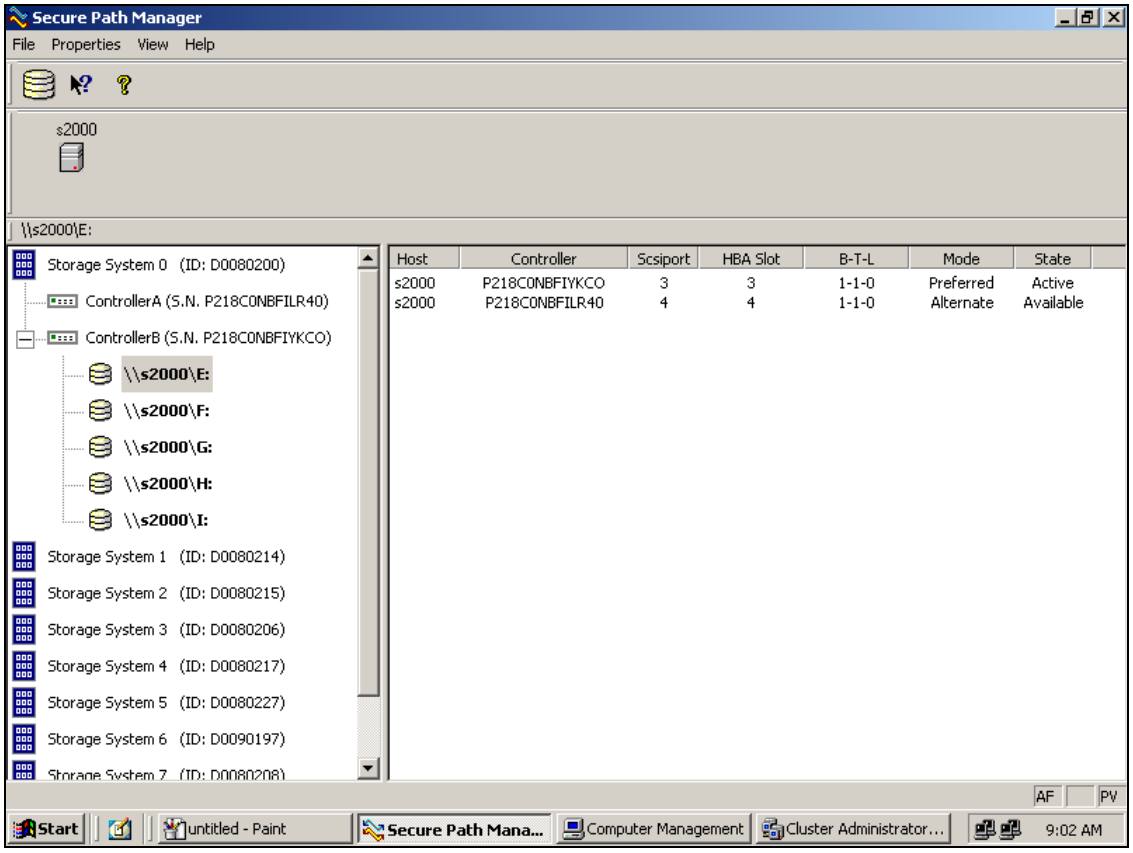

Figure 5: SPM Single Host, Multi-array Storage Profile – Physical Path View

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 periodically requests 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 the View menu by pressing **F5**, 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 updates the entire display, it can take longer to perform than a normal polling operation. How long the Refresh takes depends 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 SPM, but appears 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:

- Click the drive to highlight it in the storage system view.
- 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:

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

If the path was Alternate Available, its mode changes to alt-offline. If the path was Preferred Available, its mode changes 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:

- Click a path in the "alt-offline" or "pre-offline" mode.
- Right click to select the **Make Online** action.

If the path was alt-offline, its mode changes to Alternate Available. If the path was pre-offline, its mode changes 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:

- Click the path.
- Right click to select the **VerifyPath** action.

SPM generates a pop-up message when the verification completes to indicate the result of the operation. No state change occurs 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 a path in the FAILED State.
- Right click to select the **Repair Path** action.

If the Repair action is completed successfully the path's state changes 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 is 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 helps 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 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 6: Storage System Path Failure Detected

Storage Controller Path Failure Detected

The icon shown in Figure 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 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 performs 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 automatically detects 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 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 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 9: Storage System Failure detected

Figure 10: Storage Controller Failure detected

Figure 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, depends 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 is not detected and the path's state is not marked as FAILED until I/O operations occur.

- Is Path Verification enabled?

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

Identifying Controller Failovers

An RA4000/4100 Controller failure causes Secure Path to change the ownership of a given storageset to the surviving controller. Failover occurs 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 requires approximately two minutes per storageset to verify the integrity of all paths in the storage profile.

The Path Verification diagnostics identifies the specific failing controller in the Storage System view. Check for the failed storage controller icon shown in Figure 9. SPM shows 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 are 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 always shows the associated cluster name alongside the storageset in the Storage System view. When you highlight a storageset, SPM displays 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.

Using SpCleanUpLuns to Clean up Deleted LUNs

About SpCleanUpLuns

SpCleanUpLuns is a command line utility that cleans up LUNs shown in the failed state in Secure Path Manger (SPM). *SpCleanUpLuns* is only supported in Windows Server 2003.
Secure Path Manager sees LUNs in a failed state for one of the following reasons:

- LUNs are deleted using the Array Configuration Utility (ACU).

  In this case, HP recommends that you uninstall the devices (LUNs) from the device manager first, before deleting the devices using the Array Configuration Utility. If you do not, Secure Path Manager sees the deleted devices as failed devices with the subsystem shown in a degraded state. In such situations HP recommends using *SpCleanUpLuns* to clean up all the devices (LUNs) that are in failed state.

- When all the paths to the LUNs are removed.

  In this case, you do not need to use *SpCleanUpLuns*.

SpCleanUpLuns Commands

To run SpCleanUpLuns, choose **Programs > Secure Path > SpCleanUpLuns**. A DOS window displays. Enter *SPCleanUpLuns* commands as described in the following sections.

spcleanupluns -?

This command displays *SpCleanUpLuns* help.

Example

```
SPDriver> spcleanupluns -?
Secure Path 3.1c for RA4100 for Windows Server 2003
Lun Clean Up Utility Version 1.0.0.0
Copyright (C) Hewlett Packard Inc.
All Rights Reserved.
SPCLEANUPLUNS -d  : Deletes the LUNs in the failed state in
Secure Path.
SPCLEANUPLUNS -?  : Displays help.
```

spcleanupluns -d

This command deletes all LUNs that are currently in failed state.

Example

```
SPDriver> spcleanupuns –d

Secure Path 3.1c for RA4100 for Windows Server 2003
Lun Clean Up Utility Version 1.0.0.0
Copyright (C) Hewlett Packard Inc.
All Rights Reserved.

Do you want to clean up the failed LUNs? (y/n)y

Lun#           SCSI address    Deleted
-------------------------------------

Lun 0         (4 ,1 ,0 ,0 )    Yes
Lun 1         (4 ,1 ,0 ,1 )    Yes
Lun 2         (4 ,1 ,0 ,2 )    Yes
Lun 3         (4 ,1 ,0 ,3 )    Yes
```

Troubleshooting Secure Path Manager Connection Problems

This section provides the following Secure Path Manager network connectivity troubleshooting information:

- Client/Agent considerations
- Network considerations

If further assistance is required, please contact the account representative or call the HP 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 on page 50 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 period (.) 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.

Choose **Import LMHOSTS** 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 period 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.

Software Components

This appendix describes the following Secure Path software components included in the Secure Path software kit for Windows on RAID Array 4000/4100.

- **RaiDisk.sys** is a Windows class driver that provides the primary failover capability in the Secure Path product. RaiDisk.sys 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 and Windows 2003 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.
- **SpCleanUpLuns.exe** is a command line utility that cleans up all LUNs that Secure Path Manager considers to be in a failed state. Using *SpCleanUpLuns* is specifically required when LUNs are deleted using the Array Configuration Utility (ACU) without uninstalling it from the Device Manager.
- **Secure Path Agent** is a Windows service that communicates with the RaiDisk class 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.
- **hpscws** is a Windows filter driver for HBAs that modifies the device identification strings for the RA4100/4000 LUNs. This modification is required for **RaiDisk.sys** to recognize the RA4100/4000 LUNs.

- **rdfil.sys** is a Windows filter driver that provides support for Secure Path with Microsoft Clustered servers (MSCS).

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

glossary

This glossary defines terms used in this guide or related to this product and is not a comprehensive glossary of computer terms.

controller
A hardware device that facilitates communication between a host and one or more LUNs organized as an array.

controller states

- **Critical**–Reported for a controller pair bound in multi-bus failover mode when only one of the controllers is available. This state can mean a failed or offline condition, because the server cannot communicate with the other controller at this time.
- **Operational**–The controller is available with a good status.
- **Unknown**–The server cannot communicate with this controller.

device states
Attributes that describe the current operational condition of a device. A device can exist in the following states:

- **Critical**–Only one path remains available to the storage unit.
- **Degraded**–One or more paths are failed to the storage unit.
- **Operational**–The Secure Path device can be accessed on at least one path.
- **Unknown**–Unable to communicate with the unit. This can indicate no available path or a failed device.
- **Dead**–All paths used by this Secure Path device have failed.

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

failover
The automatic substitution of a functionally equivalent system component for a component that failed.

HBA
Host Bus Adapter. An I/O device that serves as the interface connecting a host system to the SCSI bus or SAN (Storage Area Network).

host
A computer system on which the Secure Path server software is running.

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

mode
A user-selectable parameter that specifies path behavior during nominal and failure conditions. Paths can be set to one of the following modes:

- **Preferred**–Indicates the desired I/O paths. 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 are verified.
- **Alternate**–Indicates a path is used only for device access only afteer 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 ordered 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.

path state
An attribute that describes the current operational condition of a path. A path can exist in one of the following states:

- **Active**–Currently servicing I/O requests.
- **Available**–Available on the active controller for the I/O stream.
- **Failed**–Currently unusable for the I/O stream.
- **Preferred**–indicates the path is preferred for I/O stream, across reboot.

port A
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.

profile
A Secure Path file that stores configuration limits information. The profile includes server, storage system, and failover mode information. The Secure Path Manager lets you create multiple profiles that you can apply to your systems.

SAN
Storage Area Network. A configuration of networked devices for storage.

state
An attribute that describes the current operational condition of an object. *See also* Path, Path State, Attribute, Controller States, and Device States.

target
- For parallel SCSI configurations, the target is the actual target number assigned to a device.
- For Fibre Channel configurations, a target number is assigned by a mapping function at the miniport-driver level and is derived from AL_PA (Arbitrated Loop Physical Addresses) in an FC-AL topology.
- For SAN switched fabric, a target is assigned to a WWPN. This target can have values between 16 and 125.
- For a fabric topology, target is a mapping function derived from the order of discovery according to port connections at the SAN (Storage Area Network) switch.

topology
An interconnection scheme that allows multiple servers and storage devices to communicate. Arbitrated Loop and switched fabric are examples of Fibre Channel topologies.

index

T

U

W