Compaq StorageWorks

Compaq StorageWorks Command Console Version 2.4

User Guide

First Edition (May 2001)
Part Number: AA-RFA2H-TE
Compaq Computer Corporation

Compaq StorageWorks Command Console Version 2.4
User Guide
First Edition (May 2001)
Part Number: AA-RFA2H-TE

Contents

Chapter 2
Using Command Console

Chapter 3
Setting Up Notification

Chapter 4
Interpreting Agent Email Messages

Appendix A

Using the Command Console LUN

Appendix B

Interpreting SNMP Traps

Glossary

Index

Figures

Tables

About This Guide

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

Intended Audience

This guide is intended for storage administrators. This document assumes that you have a basic understanding of storage and networks.

Documentation

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

Online Help

After you configure the software, you should refer to the online Help to learn more about this application. The online Help provides further information on using StorageWorks Command Console (SWCC) Version 2.4.

Release Notes

Look for late-breaking and supplemental information for SWCC by referring to the release notes.

In this Guide

This guide contains the following chapters and appendixes:

Chapter 1 — About the Command Console provides a description of the function and capabilities of the SWCC application.

Chapter 2 — Using Command Console provides instructions on how to use SWCC.

Chapter 3 — Setting Up Notification provides instructions on how to set up notifications on SWCC.

Chapter 4 — Interpreting Agent Email Messages provides a description of how to interpret Agent email messages.

Chapter 5 — Using Storage Windows provides instructions on how to use Storage Windows.

Chapter 6 — Integrating SWCC with Compaq Insight Manager provides instructions on how to integrate SWCC with the Compaq Insight Manager.

Chapter 7 — Troubleshooting provides instructions on how to troubleshoot SWCC.

Appendix A — Using the Command Console LUN provides instructions on how to use the SWCC LUN.

Appendix B — Interpreting SNMP Traps provides instructions on how to interpret SNMP trap messages.

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 different typeface and in uppercase
FILENAMES	File names appear in uppercase italics.
Menu Options, Command Names, Dialog Box Names	These elements appear in initial capital letters.

COMMANDS, DIRECTORY NAMES, and DRIVE NAMES	These elements appear in uppercase. [NOTE: UNIX commands are case sensitive and will not appear in uppercase]
Type	When you are instructed to *type* information, type the information **without** pressing the **Enter** key.
Enter	When you are instructed to enter information, type the information and then press the **Enter** key.

Symbols in Text

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

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

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

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

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

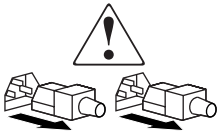
Symbols on Equipment

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

Any surface or area of the equipment marked with these symbols indicates the presence of electrical shock hazards. Enclosed area contains no operator serviceable parts.
WARNING: To reduce the risk of injury from electrical shock hazards, do not open this enclosure.

Any RJ-45 receptacle marked with these symbols indicates a Network Interface Connection.
WARNING: To reduce the risk of electrical shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.

Any surface or area of the equipment marked with these symbols indicates the presence of a hot surface or hot component. If this surface is contacted, the potential for injury exists.
WARNING: To reduce the risk of injury from a hot component, allow the surface to cool before touching.



Power Supplies or Systems marked with these symbols indicate the equipment is supplied by multiple sources of power.
WARNING: To reduce the risk of injury from electrical shock, remove all power cords to completely disconnect power from the system.

Any product or assembly marked with these symbols indicates that the component exceeds the recommended weight for one individual to handle safely.
WARNING: To reduce the risk of personal INJURY or damage to the equipment, observe local occupational health and safety requirements and guidelines for manual material handling.

Getting Help

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

Compaq Technical Support

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

In North America, call the Compaq Technical Phone Support Center at 1-800-OKCOMPAQ. This service is available 24 hours a day, 7 days a week.

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

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. Visit 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 numbers
- Product model names and numbers
- Applicable error messages
- Add-on boards or hardware
- Third-party hardware or software
- Operating system type and revision level
- Detailed, specific questions

Compaq Website

The Compaq website has latest information on this product as well as the latest drivers. Visit the Compaq Storage website at http://www.compaq.com/storage.

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

About the Command Console

What is StorageWorks Command Console?

SWCC allows you to monitor and manage the storage connected to your HS-Series controller. Command Console is a management framework with a graphical user interface (GUI) for managing StorageWorks RAID array products. It runs on Microsoft Windows NT 4.0, service pack 4 or later and Windows 2000, service pack 1. With Command Console you can configure virtual disks, receive notification of events, and monitor your storage systems.

The SWCC works with Client and Agent components. The Client is a device-specific GUI program designed for use with Command Console on the Windows platform. It provides an easy method of configuring, operating, monitoring, and troubleshooting a particular subsystem. An Agent is a companion program that is installed on a host system running a supported operating system. The host system is connected to the controllers and switches managed by SWCC. Having both the Agent and Client available allows SWCC to manage storage subsystems over a network.

Command Console Features

The Command Console contains the following features:

- Manages StorageWorks RAID Arrays over a serial port, SCSI bus, or TCP/IP network.
- Configures RAID arrays using menus, icons, and system views.
- Provides an Explorer-like Navigation Window and right click on mouse for properties.
- Configures arrays from files. Array configurations can be saved as files and used as backup or to automatically configure other arrays.

- Upgrades subsystem software.
- Monitors subsystems. Subsystem monitoring includes power, cooling, temperature, device, controller, and cache monitoring.
- Protects your data and configuration with password protection option.
- Interfaces with Windows NT or Windows 2000 logging capability on storage systems connected to Windows NT or Windows 2000 servers (not clients), listing RAID array events in the NT event log.
- Notifies you of subsystem problems via pager.

Components of SWCC

SWCC includes:

- Command Console - The Command Console consists of the Navigation Tree, Navigation Window, Asynchronous Event Service and Pager Notification. For an explanation of Pager Notification, see the section titled Setting Up Notification in Chapter 3.
- HS-Series Controller Client - The HS-Series Controller Client provides a Storage Window that displays detailed information about a specific subsystem. From the Storage Window, you can manage your subsystem, for example, creating virtual disks.

  For information on using features in a Storage Window, see the section titled Using Storage Windows in Chapter 5.

  To access the Storage Window, do the following:

  a. Click *Start* > *Programs* > *Command Console* > *StorageWorks CC HSxxx*. (serial, SCSI, and network connections)
     OR
     Double click the Storage Window icon in the Navigation Tree. (network connection only)
- CLI Window -You can monitor and configure your subsystem by typing commands into the Command Line Interpreter (CLI) Window. The CLI offers the same functionality as the Storage Window. For more information, refer to the *Compaq StorageWorks HSG80 Array Controller ACS Version 8.6 CLI Reference Guide.* You can access the CLI window by two methods:

  To access the CLI Window, do one of the following:

a. Click *Start* > *Programs* > *Command Console* > *StorageWorks CC CLI Window.* (serial, SCSI, and network connections)
OR
Double click the CLI Window icon in the Navigation Tree. (network connection only)Click *Start,* then select *Programs.*

- HS-Series Agent performs the following:
  - Obtains the status of the storage connected to the controller.
  - Passes the status of the devices connected to the controller to the Navigation Tree, which passes the information to the Storage Window.
  - Passes the status of the devices connected to the controller to the Event Viewer.
  - Provides email notification. This feature is not available on Novell NetWare, Windows 2000, or Windows NT (4.0 with Service Pack 4 or later).

Refer to Table 1–1 for a summary of the SWCC features and required components.

Table 1–1 SWCC Features and Components

Features	Agent Required?	Client Required?
Able to create storagesets	Yes	Yes
Able to monitor many subsystems at once	Yes	Yes
Event logging	Yes	No
Email notification (Does not apply to Agents running on Novell NetWare, Windows NT 4.0, or Windows 2000)	Yes	No
Pager notification	Yes	Yes

Client and Agent Versions

SWCC uses different clients and agents along with the Command Console to provide storage management over a network. There is a single version of the Command Console that is used with all device-specific clients. There is a unique client for each supported HS-Series controller. There is an agent for each supported operating system though each agent is compatible with all supported controllers.

See the current versions of the Command Console, Agent, CLI Window, and device-specific clients in Table 1–2.

Table 1–2 SWCC Component Versions

SWCC Component	Version
Command Console (Storage Window Manager)	V2.2.0
Agent	V2.3.2
SWCC CLI Window	V2.0.0
HSG80ACS85 Storage Window	V2.4.0
HSG80 Storage Window	V2.1.0
HSG60 Storage Window	V2.4.0
HSZ80 Storage Window	V2.3.0
HSJ80 Storage Window	V2.3.0
HSZ Storage Window	V2.3.0
HSJ Storage Window	V2.0.0
HSD Storage Window	V2.0.0

Command Console Client Minimum Hardware and Software Requirements

The minimum requirements to run the Command Console client properly are listed in Table 1–3.

Table 1–3 Minimum Hardware and Software Requirements

Item	Requirements
Management Station	Suggested minimum of a Pentium class system with 64 MB of RAM memory
Operating System	Windows NT 4.0 (Intel) Service Pack 4 or later, and Windows 2000 Service Pack 1 or later
Monitor	VGA at 800x600 resolution, minimum
Modem	Hayes-compatible (for event notification)
Serial Port	RS-232 (for local connection)
Network Adapter	TCP/IP-compatible network card (for distributed systems only)
Controller Compatibility	HSG80, HSG60, HSZ80, HSZ70, HSZ50, HSZ40, HSZ20, HSJ80, HSJ50, HSJ40, HSJ30, HSD50, HSD30
Host Software	ASPI SCSI driver required for host port virtual terminal connection (Windows NT only)

Network Specifications

Command Console is a terabyte-class RAID Array manager. Fully scalable, Command Console can manage a single, locally connected RAID array or RAID arrays in a multi-node, TCP/IP network environment. Command Console can support any number of Clients and Agents in a distributed environment.

Connections Supported by SWCC

SWCC manages storage by using Storage Windows. Storage Windows are GUI-enabled, device-specific clients that communicate with storage devices either directly or through an agent. Storage Windows are used to configure and monitor storage arrays. An agent is connected to storage controllers which it configures and monitors. There are several different types of connections used by the clients to communicate with storage controllers and with agents.

SWCC provides storage management over the following connections, as listed in Table 1–4:

- Direct Serial connection
- SCSI connection
- Storage Area Network (SAN) and TCP/IP network

Table 1–4 SWCC Connections for HS-Series Controllers

Connection	Agent Required?
SAN and TCP/IP network connection	Yes
Direct serial connection	No*
SCSI connection**	No**

* If you do not install Agent, you cannot use the Navigation Tree or pager notification.

**SCSI is only available for HSZ-Series controllers. SCSI over Fibre Channel is available with HSG60 and HSG80 controllers.

IMPORTANT: SWCC does not support the (Dynamic Host Configuration Protocol (DHCP) or the Windows Internet Name Service (WINS); however, you can still use these protocols on systems that do not run Command Console.
To determine whether your system is using DHCP or WINS on Windows 2000 or Windows NT 4.0:

- Right click Network Neighborhood on the desktop.
- Select *Properties*.
- Click the Protocols tab.
- Select TCP/IP, then click *Properties*. The Microsoft TCP/IP Properties window appears.

SAN and TCP/IP network connection

By using a network connection as shown in Figure 1–1, you can configure and monitor your storage subsystem from anywhere on your Local Area Network (LAN). If your have a Wide Area Network (WAN) or a connection to the Internet, you can monitor your subsystem with TCP/IP.

SWCC can include any number of Clients and Agents in a network. However, it is suggested that you install only one HS-Series Agent (except for the HSZ22 Agent) on the computer that has a connection to the HS-Series controller.

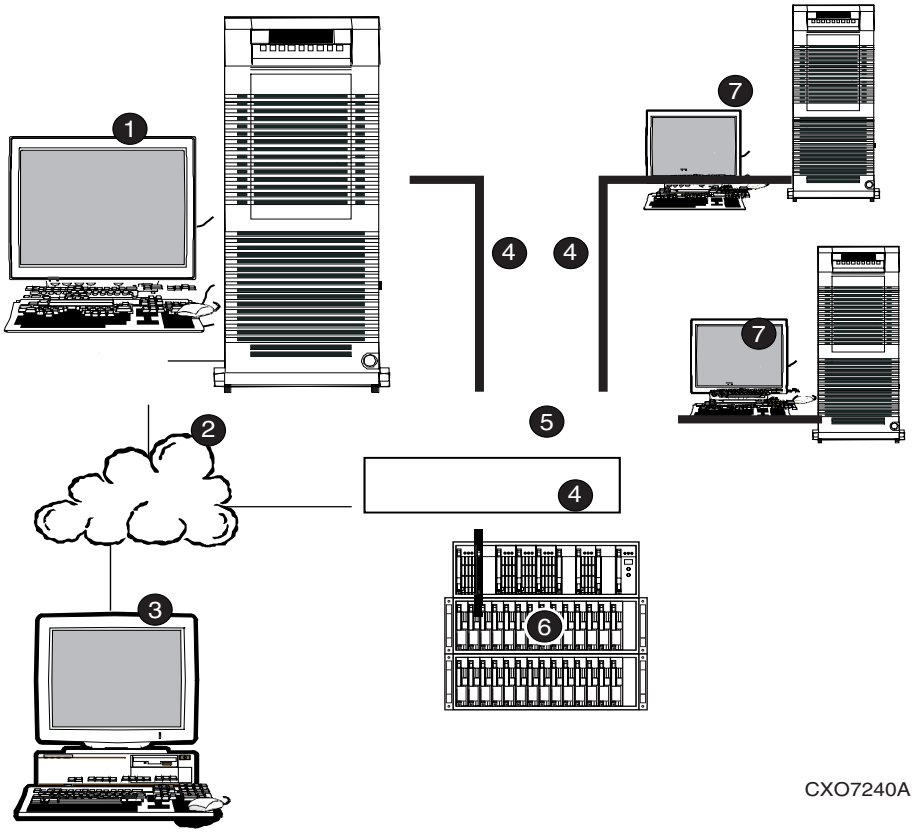


Figure 1–1. SAN and TCP/IP network connection

❶ Agent System (has Agent software)

❷ TCP/IP Network

❸ Client System (has Client software)

❹ Fibre Channel cable

❺ Hub or Switch

❻ Storage system

❼ Servers

Local Serial Port Connection

A local serial port connection uses only the Storage Window to manage your storage subsystems. The client system is connected to the subsystem by a serial connection, as shown in Figure 1–2.

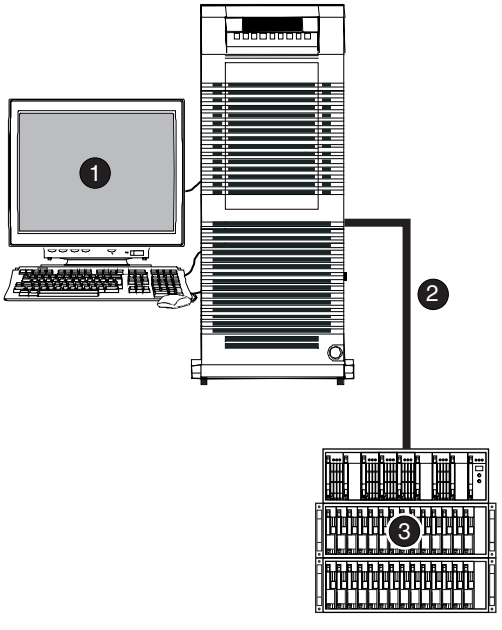


Figure 1–2. Local serial port connection

❶ Client system

❷ Serial connection

❸ Storage system

SCSI Connection

A SCSI connection over a SCSI bus or using the Fibre Channel bus, as shown in Figure 1–3, uses only the Storage Window to manage your storage system. This connection is supported by the HSZ-Series controller for a SCSI bus. The HSG60 and HSG80 controllers support the SCSI over Fibre Channel bus connection.

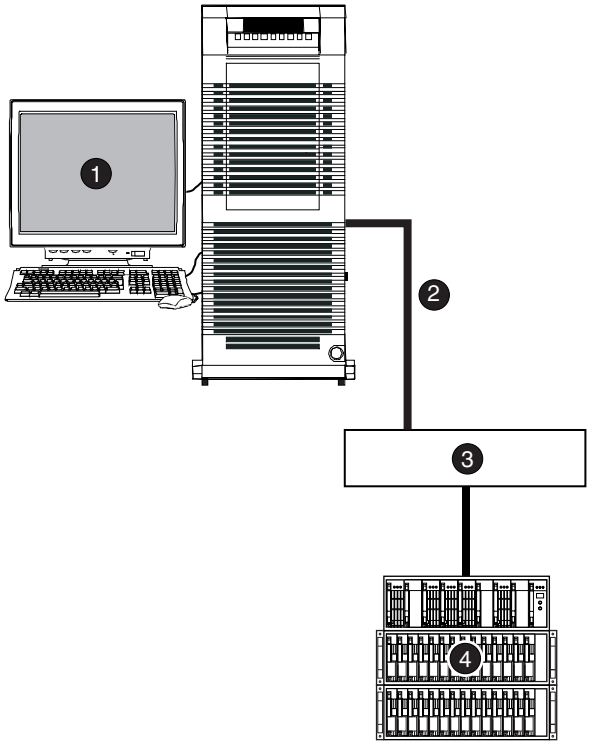


Figure 1–3. SCSI connection using Fibre Channel cable

❶ Client system that has the Storage Window

❷ Fibre Channel cable (using SCSI connection)

❸ Hub or Switch

❹ Storage system

Accessing the Storage Window

You can access the HS-Series Storage Window from the Start menu. You can connect the Storage Window to storage over a serial connection, a SCSI connection, or a TCP/IP network.

Before you can make either a SCSI or a network connection, you must have one of the following:

- A virtual disk created on the subsystem
- Command Console LUN (CCL) enabled

For more information about:

- Creating a virtual disk, see the section titled Creating Virtual Disks in Chapter 5.
- Enabling and disabling the Command Console LUN, see Appendix A, Using the Command Console LUN.
- Accessing the Storage Window from the Navigation Tree, see the section titled Managing Storage Subsystems from the Navigation Tree in Chapter 2.

Serial Connections

The simplest connection to a subsystem is a direct cable connection from the Client's host system to a serial port on the subsystem. The serial connection is often used to set the initial configuration of a storage subsystem. This initial configuration can then allow a SCSI or network connection to the subsystem.

A direct serial connection to a subsystem does not provide as much functionality as a network connection. The agent is bypassed so that any agent-related function is not available. These functions include event logging and email notification. The Navigation Tree is not available with a direct serial connection.

To set up a serial connection:

1. Click *Start* > *Programs* > *Command Console* > *StorageWorks CC HSxxx*. The Connection Selection window appears, as shown in Figure 1–4.

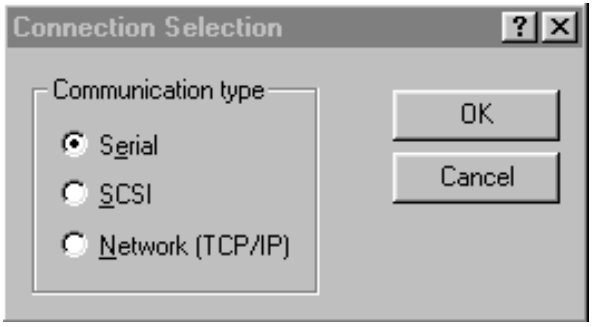


Figure 1–4. Connection Selection dialog box

2. When the Connection Selection window appears, select Serial and then click *OK*. The Connect Serial window appears, as shown in Figure 1–5.

3. From the drop-down menu, select the COM port used by the RAID HS-Series controller.
4. Select a baud rate, a Subsystem Physical View, and a Subsystem Grid View. Click *Connect*. When the Storage Window appears, you are connected to your subsystem.

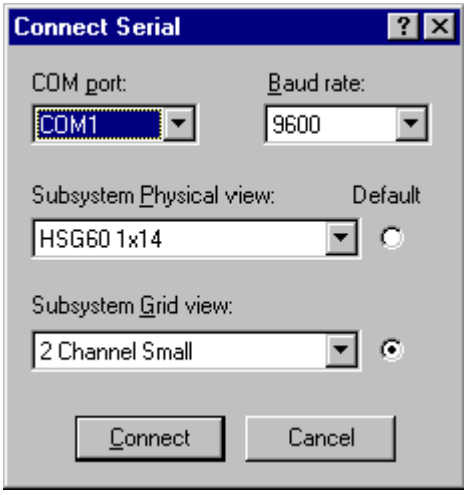


Figure 1–5. Connect Serial window

SCSI Connections

The SCSI connection uses the SCSI bus or Fibre Channel bus that is the primary data channel for the storage subsystem. The amount of management information that passes between the Storage Window and the subsystem is small compared to the amount of data moved by a typical storage request.

Like the direct serial connection the SCSI connection does not use an agent. The SCSI connection only supports a Storage Window or CLI Window without a Navigation Tree. There is no event logging or pager notification with a SCSI connection. Establishing a SCSI connection requires that a Command Console LUN or a virtual disk be configured on the storage subsystem.

1. Click *Start* > *Programs* > *Command Console* > *StorageWorks CC HSxxx*.
2. When the Connection Selection dialog box displays, select the *SCSI* option. The SCSI Setup window appears, as shown in Figure 1–6.

3. Select a drive mapped to the subsystem, then click *Connect.* After a brief delay, Command Console connects to the storage subsystem and displays the corresponding Storage Window.

.

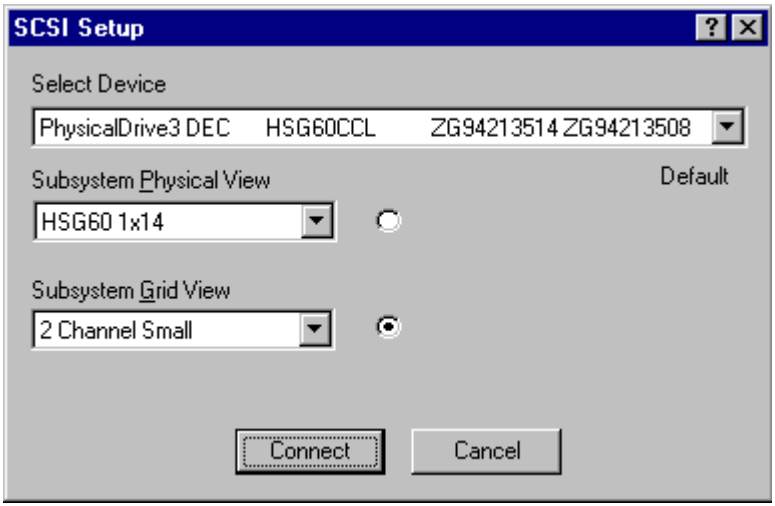


Figure 1–6. SCSI Setup window

Network Connections

Using SWCC with a network connection provides more features and flexibility for managing storage subsystems than serial or SCSI connections. A network connection between a client and agent supports the use of the Navigation Tree, allowing for the management of multiple subsystems from a single application. The use of an agent enables event logging on the agent host and also email and pager notification for subsystem events.

A network connection requires that an agent be installed on a host connected to the storage subsystem. Establishing a network connection requires that a Command Console LUN or a virtual disk be configured on the storage subsystem. If the storage subsystem is not properly preconfigured then a serial connection must be made to enable the Command Console LUN or to create a virtual disk.

To use SWCC to manage the HS-Series controller over a network, install the Command Console, the HS-Series device-specific Client (Storage Window), and the HS-Series Agent. The Command Console and the HS-Series Client are installed together.

NOTE: The HSZ22 does not use the same Agent used for the other HS-Series controllers.

To set up SWCC to manage the HS-Series controller over a network:

1. Click *Start* > *Programs* > *Command Console* > *StorageWorks CC HSxxx*. The Client displays the Connection Selection window.
2. Select the Network (TCP/IP). The Connect Network (TCP/IP) window appears, as shown in Figure 1–7.
3. Enter the host IP name or address in the text box, then click *Detect Subsystems.* Client locates the subsystem connected to the host.
4. Select the subsystem, then click *Connect.* The Client displays the Storage Window.

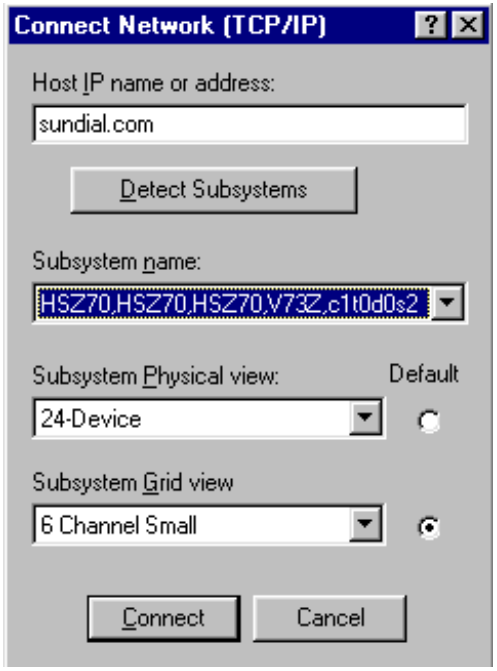


Figure 1–7. Connect Network (TCP/IP) window

Chapter 2

Using Command Console

Using the Navigation Tree

The Navigation Tree appears in the Navigation Window. The Navigation Tree lets you view the status of all your storage at once, as shown in Figure 2–1. Note that some items shown in this Navigation Tree may not represent the software in your release.

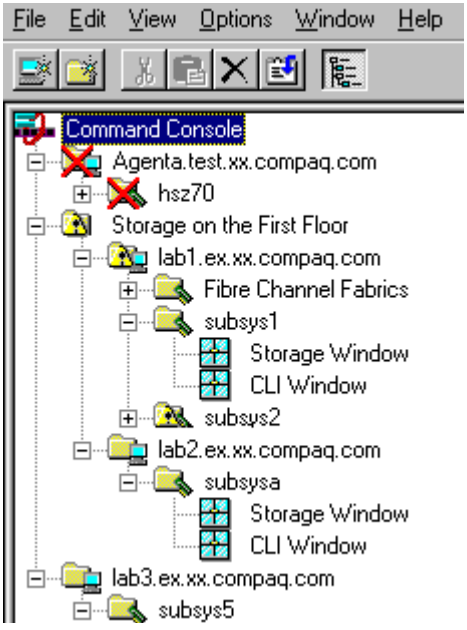


Figure 2–1. An example of the Navigation Tree

Adding an Storage Subsystem to the Navigation Tree

The Navigation Tree allows you to manage your storage over the network from the Storage Window. If you plan to use pager notification, you must add the storage subsystem to the Navigation Tree.

To add the storage subsystem to the Navigation Tree:

1. Verify that you have properly installed and configured the HS-Series Agent on the storage subsystem host. For more information, refer to the installation and configuration guide for your operating system.
2. To display the Navigation Window, click *Start* > *Programs* > *Command Console* > *StorageWorks Command Console*.
3. Click *File* > *Add System*. The Add System window appears.
4. Type the host name or its TCP/IP address and click *Apply.*
5. Click *Close*.
6. Click the plus sign (+) to expand the host icon. When expanded, the Navigation Window appears as an icon for the storage subsystem. To access the Storage Window for the subsystem, double click the Storage Window icon.

Managing Storage Subsystems from the Navigation Tree

You can manage a storage subsystem from the Navigation Tree by double clicking the Storage Window or CLI Window icon

To access a subsystem management window:

1. Double click the folder for the storage subsystem. An icon appears underneath the folder.
2. Double click the Storage Window or CLI Window icon for the subsystem.

Organizing Your Storage in the Navigation Tree

After you add systems to the Navigation Tree, you can organize your storage in folders:

- You can place folders under the Command Console root or under another general folder in the Navigation Window.
- You can use folders to group systems and other general folders. Note that you cannot use folders to group controllers.

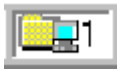
For example, in Figure 2–1, the general folder *Storage on the First floor* was created and two agent systems were placed in the folder. If a system in the folder is at a critical state, the status of the folder displays the same critical state.

> **NOTE:** For a description of the Navigation Window, refer to the "Quick Tour" in the introduction of the Command Console Client online Help.

About the Navigation Tree Icons

The icons in the Navigation Tree that are listed in Table 2–1, change to show system status. The Navigation Window status bar, located in the lower-right corner, summarizes the host system connection status.

Table 2–1 Description of Icons in Navigation Window Status Bar

Icon	Description
	Indicates the number of disconnected systems
	Indicates the number of fully functional systems
	Indicates the number of degraded systems
	Indicates a critically failed system

About the Asynchronous Event Service

The Asynchronous Event Service (AES) does the following:

- Runs in the background as a service that provides status updates of the subsystems to its client system. For a client system to receive updates, it must run AES.

- Passes the trap (message) to the Navigation Tree. The Navigation Tree, in turn, passes the trap to the appropriate Storage Window or Fabric Window. When a trap provides information about a status change in a subsystem, one or more of the icons in the Navigation Tree change color.
- Send traps to pagers. To activate this feature, you must predefine each pager number in the *User Profile* section of the Event Notification menu in the Navigation Window.

  NOTE: Refer to Command Console's online Help for the latest information about how to diagnose problems that can occur when sending pages. Help provides instructions on how to put AES into a debug mode.

AES Functionality

You can modify whether AES starts at boot time. You can also manually stop or start AES. However, you must run AES to receive pager notification of faults and to provide updates to the Navigation Tree, Storage Windows, and Event Viewer. If you stop AES, the Client software will stop the following functionality:

- Updates to the Navigation Tree and Storage Windows
- Updates from AES in the Application Log of the Event Viewer
- Notifying pagers if a fault occurs

To Stop or Start AES

From Windows NT

To stop or start AES manually:

1. Double click *Services* in Control Panel.
2. Click the *AsyncEventSvc* entry.
3. Click *Stop* or *Start*, then click *Close*.

To disable AES from starting automatically when your system boots, change the startup option to manual in the Services window. Use the following steps:

1. Double click *Services* in Control Panel.
2. Double click the *AsyncEventSvc* entry. The Services window appears.
3. Select *Manual* under Startup Type, and click *OK*.

From Windows 2000

To stop or start AES manually:

1. Click *Start* > *Settings* > *Control Panel* > *Administrative Tools* > *Component Services*.
2. Under Console Root, select *Services (Local).*
3. Under Services (Local), right click *AsyncEventSvc*.
4. Click *Stop* or *Start*.

To disable the automatic start of AES at system boot, change the startup option to manual:

1. Click *Start* > *Settings* > *Control Panel* > *Administrative Tools* > *Component Services*.
2. Under Console Root, select *Services (Local).*
3. Under Services (Local), right click *AsyncEventSvc*.
4. From the drop-down menu, select *Properties*. The AsyncEventSvc Properties (Local Computer) window appears.
5. Under the General tab, select *Manual* from the Startup Type drop-down menu.
6. Click *OK*.

Chapter 3

Setting Up Notification

Required Components for Notification

Table 3–1 lists the notification options available with SWCC and the components required for each option.

Table 3–1 Required Components for Notification

Notification Option	Required Components
Navigation Tree	Client and Agent
Pager	Client and Agent
Email notification (applies to certain agents)	Agent
Event logging	Agent
SWCC with third-party storage management program	Agent and third-party storage management program

Setting Up Pager Notification

You can set up Command Console to notify you by pager when a critical event occurs. This feature works with alphanumeric and numeric pagers. You can configure this feature to send pages to multiple people at various times. For example, if several people monitor your network in shifts, you can configure this feature so the software pages only people working the current shift.

To receive pages, the following must occur:

- The AES must be running on the client system on which you set up the pager notification.
- The Agent must be running.
- The client system must be added to the Agent's list of client system entries.
- In the Agent's list of client system entries, you must select the TCP/IP notification scheme for your client system.
- You must add the Agent system to the Navigation Tree of the client system on which you set up pager notification.

NOTE: Pager notification uses the Telocator Alphanumeric Protocol (TAP) adopted in 1988 by the Personal Communications Industry Association (PCIA). Verify that your paging company uses this protocol.

Table 3–2 lists and describes the steps to use to set up pager notification. Hyperlinks to chapter sections that provide detailed information for each step are included in the table.

Table 3–2 Setting Up Pager Notification

Step	Description	Refer to Section
1	Numeric Pagers only - assign pager codes to host systems and controllers.	Setting Up Pager Codes.
2	Set up user profiles.	Setting Up User Profiles.
3	Set up notification lists.	Setting Up Notification Lists.
4	Set up modem and polling intervals.	Setting Up Modem and Polling Preferences.
5	Associate systems and controllers with notification list.	Associating Systems and Subsystems with Notification Lists.

Setting Up Pager Codes

Numeric pager support lets you receive notification about critical events.

A numeric pager usually has three fields separated by hyphens. The first field signifies the area code, the second field signifies the exchange, and the third field signifies the four-digit extension.

A page from Command Console is structured as follows:

- First field is a three-digit number for the host system.

- Second field is a three-digit number for the subsystem.
- Last field is a four-digit code for the critical event.

To set up pager codes, first assign a three-digit code for each host system, then assign another three-digit code for each subsystem controller connected to that host. The last four digits are pre-assigned. You can change them.

To Assign a Pager Code to a Host System:

1. Click a host system in the Navigation Window.
2. Click *File* > *Properties*.
3. Click the Event Notification tab.
4. Enter a three-digit number in the field "Pager identification number." Avoid entering a number that may be mistaken for an area code.

To Assign a Pager Code to a Subsystem:

1. Click a subsystem controller in the Navigation Window.
2. Click *File* > *Properties*.
3. Click the Event Notification tab.
4. Enter a three-digit number in the field "Pager identification number."

To View or Change a Pager Code for a Critical Event:

1. Click *Options* > *Event Notification* > *Pager Codes*.
2. Click the code you want to edit, then click *Edit*.
3. Type the new pager code in the Edit field.

The default pager codes are listed in Table 3–3.

Table 3–3 Default Pager Codes

Critical Event	Code	Notes
Disk Fault	1000	Physical device failure
Power Supply Fault	1002	
Fan Fault	1003	
Battery Fault	1004	

Table 3–3 Default Pager Codes (Continued)

Critical Event	Code	Notes
Temperature Fault	1005	
Controller Fault	1006	The controller detected an internal fault
Communication Fault	1007	Agent cannot talk to the subsystem.
Other controller fault	1008	One controller is reporting a fault on the other.
External fault	1009	
LUN Fault	1010	Virtual disk failure

NOTE: All codes are numeric-only; alphanumeric pager codes are not supported.

Setting Up User Profiles

1. Click *Options* > *Event Notification* > *User Profiles.*
2. Click *New.*
3. Type a name. If you want, you can also enter a description.
4. Click the Pager tab.
5. Select Enabled.
6. Enter the phone number for your pager in the Pager Number field.
7. Select Alphanumeric for alphanumeric paging.
8. Type the pager identification number (PIN). (This is required for alphanumeric pagers). If your numeric pager does not require a PIN, leave the field blank. For example, this field must be blank for numeric pagers that are assigned a unique telephone number.
9. Type the start and end times in the format HH:MM, using a 24-hour clock, for example, 08:00 as the start time and 17:00 as the end time. Set both fields to 00:00 for 24-hour a day notification.

Keep in mind the following:

- If you dial a code to access an outside number, the code must precede the phone number in the pager number field.
- Do not use commas with alphanumeric pagers, except to access an outside line.

- Alphanumeric pagers require you to supply the paging service provider's TAP service modem number in the pager number field.
- Optionally, you can use one or more commas to specify a two-second wait interval for numeric pager numbers. Each comma causes the pager dialer to wait two seconds before sending the PIN to the paging company. You may need to add more commas to make the Command Console pause long enough for the pager company greeting to complete.
- Not every paging company requires a PIN. If your pager is assigned a unique phone number for calling the paging company, do not enter a PIN.
- Alphanumeric pagers require a PIN.
- Refer to your pager documentation to determine which special characters are supported.

Figure 3–1 shows a sample user profile for an alphanumeric pager, and Figure 3–2 shows a sample user profile for a numeric pager.

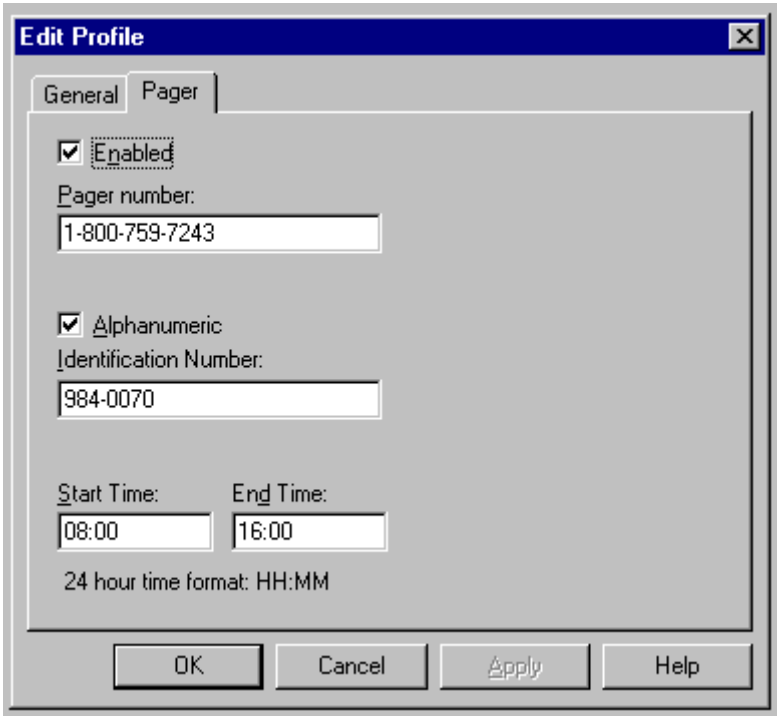


Figure 3–1. Sample user profile – alphanumeric paging

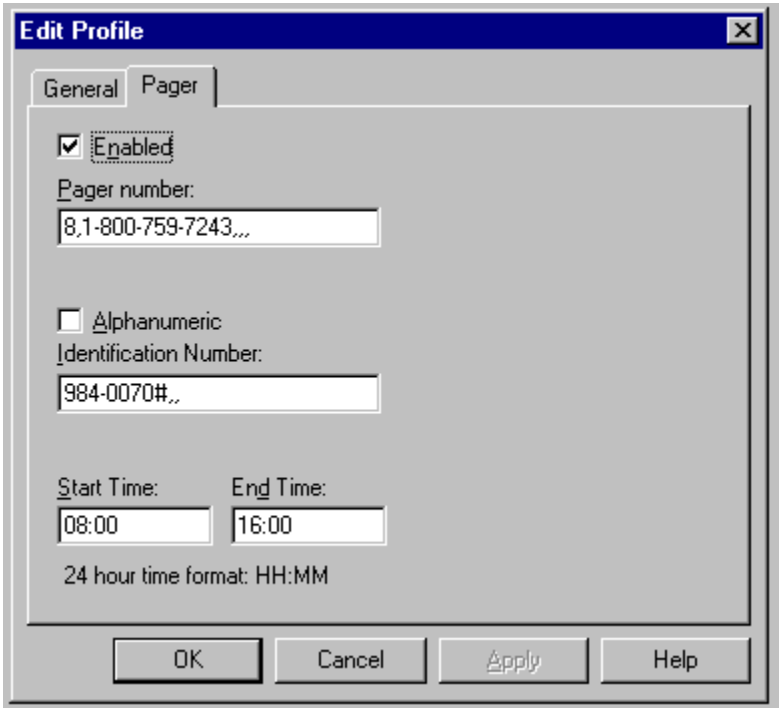


Figure 3–2. Sample user profile – numeric paging

NOTE: The commas in the Identification Number field represent two-second wait intervals.

Setting Up Notification Lists

Use notification lists to notify groups about critical events. Be sure to first create a user profile for each user in the group because you cannot add a user without an existing user profile to a notification list. Then, use the Properties pages to associate notification lists with systems and subsystem critical events.

1. Click *Options* > *Event Notification* > *Notification List.*
2. Click *New* and enter a name for the new notification list.
3. Write a brief description of the list (optional).
4. Add members to the list by clicking the check box next to each name.

Setting Up Modem and Polling Preferences

The subsystem-polling interval is the frequency at which the Client pings an Agent to determine if it is running.

1. Click *Options* > *Preferences.*
2. Type the number of hours or minutes in the subsystem polling interval field. The default-polling interval is 30 minutes.
3. Select the COM port in your computer that your modem uses.
4. For alphanumeric pagers, select the baud rate of your paging service provider's TAP modem. Typically, this is 1200 baud.

Associating Systems and Subsystems with Notification Lists

Before you can associate a system or controller with a notification list, You must first create a notification list. See Setting Up Notification Lists.

To associate a host system or a subsystem with a notification list for the purpose of paging a group if a critical event occurs:

1. Click a host system or a subsystem in the Navigation Window.
2. Click *File* > *Properties*.
3. Click the Event Notification tab.
4. Select a notification list from the drop-down list.

Using SWCC with a Third-Party Storage Management Program

To use SWCC with a third-party storage management program:

1. Add the name of the computer on which the third-party storage management program resides to the Agent's list of client system entries. Select SNMP as the notification scheme. The Agent sends SNMP traps to every client system on its list.

   For more information on how to add client systems, see the Installation and Configuration Guide for your Agent.

2. Use the compiler that came with your third-party storage management program to compile the Management Information Base (MIB) file, *HS-agent.mib* in this kit.

NOTE: Depending on the third-party software, you may need to perform additional steps. Refer to the third-party storage management program documentation.

Using Event Logging on the Client System to Monitor Your Subsystem

The Agent can place SNMP and TCP/IP traps in the Application Log of Event Viewer, which is a part of Windows NT and Windows 2000. The HS-Series Agent collects events from the controllers and lists the events under the source, AsyncEventSvc. If the Agent is installed on Windows NT and Windows 2000, you can locate its entries in the Application Log by looking for `steam` under the Source column.

For a client system to receive event logs from an HS-Series Agent on another computer:

- The client system must appear on the Agent's list of client system entries and TCP/IP must be selected as a notification scheme.
- The AES must be running on the client system.
- Agent must be running.

To access Event Viewer:

- Windows NT 4.0 – *(Start > Programs > Administrative Tools > Event Viewer)* to access the Application Log, select *Application* from the Log menu.
- Windows 2000 – *(Settings > Control Panel > Administrative Tools > Event Viewer)* to access the Application Log, select *Application Log* in the Tree panel.

For more information about SNMP traps, see Chapter 5, Using Storage Windows.

Chapter 4

Interpreting Agent Email Messages

NOTE: This chapter does not apply to the HS-Series Agents running on Novell NetWare, Windows NT 4.0, or Windows 2000.

Most of the information in this chapter pertains to the event information email messages that the RaidManager agent sends when an event occurs. If the Agent email notification feature is enabled when a RAID system event occurs, the Agent emails notification to the specified email addresses. A storage system event can be a change in the state of a physical storage device, of a logical storage unit, or of a component of the physical enclosure.

The message specifies the name of the host to which the RAID array reporting the event is connected. The message states the severity of the problem as one of these three levels:

- Critical
- Warning
- Informational

The email message appears in the following format:

```
----------------
From RaidManager Tue Oct  6 15:59:59 1998
Date: Tue, 6 Oct 1998 15:59:58 -0500 (EST)
From: RaidManager

This is an automatic message from your StorageWorks
RAID Agent, steamd. The following message was just received.
Please check your syslog files and RAID box!
Hostname: Suncity
CRITICAL: Validation failed - Unauthorized client (shr-dhcp-24-188.shr.dec.com, access level:
-1); connection refused  (SP_TCP: ClientConnect)
```

```
End Of Automatic Message.
--------------------
```

About Event Information Fields

Event information messages report on the state of the RAID system. The event information fields appear in the line following the problem severity level.

Example:

```
WARNING:-
Suncity HSG60 12000000000 HSG60 disks(disk21100:2) (SP_MONITOR: MonitorSubsys)
     \       \           \
      \       \           \
      (1)     (2)         (3)
```

Use the following information to help you to understand event information fields:

1. Host Name - the name of the host to which the RAID experiencing the event is connected.
2. Storage System - where the problem occurred.
3. State Change - the specified component of the storage system. This is an 11-digit field that provides important information about the status of your RAID Array.

Mapping State Change Digits to RAID System Components

Each of the 11 digits in the state change field can be mapped to a RAID system component. Table 4–1 lists the digits and their relationship.

Table 4–1 State Change Digit Position and Corresponding RAID System Component

State Change Digit Position	Corresponding RAID System Component
1	Overall RAID System
2	Disks
3	Power Supply
4	Fans
5	Battery
6	Temperature
7	This Controller
8	Communications LUN
9	Other Controllers
10	External Factors
11	Logical Units

The First Digit of the State Change Field (Overall RAID System)

The first digit in the state change field reports state changes in the overall RAID system.

Example:

```
WARNING: -
Suncity HSZ70 12000000000 HSZ70 disks(disk21100:2)(SP_MONITOR: MonitorSubsys)
```

The first digit can have one of two values:

0 – Everything is fine.
1 – Something has changed state.

The Second Digit of the State Change Field (Disks)

The second digit of the state change field reports state changes in disks.

Example:

```
WARNING: -
Suncity HSG70 122000000000 HSG70 disks(disk21100:2)(SP_MONITOR: MonitorSubsys)
```

This digit can have one of three values:

0 – Everything is fine.
1 – Drive went from bad to good.
2 – Drive went from good to bad.

In this example, a value of 2 is displayed in the disk digit position, indicating that a drive went from good to bad.

The disk name (in parentheses) follows, in the format:

disk_name:state

where *disk_name* is the name of the disk and *state* can be either of the following:

1 – Disk went from bad to good.
2 – Disk went from good to bad.

In this example, the failed drive is disk21100.

The Third Digit of the State Change Field (Power Supply)

The third digit of the state change field reports state changes in the power supply.

Example:

```
WARNING: -
Suncity HSG80 102200000000 HSG80 pwr(0:1:2) (SP_MONITOR: MonitorSubsys)
```

The third digit can have one of three values:

0 – Everything is fine.
1 – Power supply went from bad to good.
2 – Power supply went from good to bad.

The position (in parentheses) of the failed power supply usually follows. Three numbers indicate the position in the format:

cabinet_number:power_position:state

where *cabinet_number* is the cabinet ID from 0 to 1, the *power-position* is the power supply location (1 or 2), and *state* is one of the following:

1 – Power supply went from bad to good.
2 – Power supply went from good to bad.
3 – Power supply is not present.

In this example, the power supply in position 1 of cabinet 0 (main cabinet) went from good to bad.

The Fourth Digit of the State Change Field (Fans)

The fourth digit of the state change field reports state changes in fans.

Example:

```
WARNING: -
Suncity HSG70 100220000000 HSG70 fans(0:A:2)  (SP_MONITOR: MonitorSubsys)
```

The fourth digit can have one of three values:

0 – Everything is fine.
1 – Fan state went from bad to good.
2 – Fan state went from good to bad.

The position (in parentheses) of the fan follows, in the format:

cabinet_number:fan_position:state

where *cabinet_number* is the cabinet ID from 0 to 1, *fan_position* is the position of the fan, and *state* is either of the following:

1 – Fan went from bad to good.
2 – Fan went from good to bad.

In this example, a fan failure occurred in cabinet 0, the main cabinet.

The Fifth Digit of the State Change Field (Battery)

The fifth digit reports battery state change.

Example:

```
WARNING: -
Suncity HSG70 100020000000 HSG70 batt(6:fail)  (SP_MONITOR: MonitorSubsys)
```

The fifth digit can have one of three values:

0 – Everything is fine.
1 – Battery state went from bad to good.
2 – Battery state went from good to bad.

The details of the battery failure follow in parentheses, in the format:

controller_id:state

where *controller_id* is the SCSI ID of the reporting controller (in other words, the cache battery failed for the other controller), and *state* is one of the following:

Good – Battery is good.
Low – Battery voltage is low.
Fail – Battery has failed.

In this example, the cache battery for the controller with SCSI ID 6 failed.

The Sixth Digit of the State Change Field (Temperature)

The sixth digit of the state change field reports temperature state changes.

Example:

```
WARNING: -
Suncity HSG70 100002000000 HSG70 temp(0:2:2)  (SP_MONITOR: Monitor_Subsys)
```

The sixth digit can have one of three values:

0 – Everything is fine.
1 – Temperature state went from bad to good.
2 – Temperature state went from good to bad.

The details regarding the temperature change follow in parentheses, in the format:

cabinet_number:sensor_type:state

where *cabinet_number* is the cabinet ID from 0-1, *sensor_type* is the EMU sensor (sensor 1 or sensor 2), and *state* is either of the following:

1 – Temperature went from bad to good.
2 – Temperature went from good to bad.

In this example, an adverse temperature change is detected by sensor 2 of the main cabinet.

The Seventh Digit of the State Change Field (This_Controller)

The seventh digit reports state changes in This_Controller.

NOTE: This value is always 0 for a dual redundant configuration.

Example:

Suncity HSG70 1000000**2**000 HSG70 (SP_MONITOR: MonitorSubsys)

This digit can have one of two values:

0 – Everything is fine.
1 – Failure of the controller in a single-controller configuration.

The Eighth Digit of the State Change Field (Communications LUN)

The eighth digit reports the state changes in the communications LUN.

Example:

CRITICAL: - Suncity HSG70 1000000**2**000 HSG70 (SP_MONITOR: MonitorSubsys)

CRITICAL: Unable to open device - hdisk1 (SP_MONITOR: MonitorSubsys)

This digit can have one of three values:

0 – Everything is fine.
1 – Communications LUN is available to the host machine.
2 – Communications LUN is not available to the host machine.

In this example, two mail messages appear. The first message indicates that a communications LUN changed state from good to bad. The second message indicates that the Agent is unable to open the communications LUN for monitoring the RAID system.

The Ninth Digit of the State Change Field (Other_Controller)

The ninth digit reports states changes in the Other_Controller.

Example:

```
WARNING: -
Suncity HSG70 1000000020 0 HSG70  (SP_MONITOR: MonitorSubsys)
                         ⬆
```

This value never changes for a single controller configuration. It always changes if either controller in a dual redundant configuration fails.

This digit can have one of three values:

0 – Everything is fine.
1 – Both controllers are functioning.
2 – One of the two controllers failed.

Physically inspect the controllers to verify which one failed, as indicated by a solid green indicator light (not blinking).

The 10th Digit of the State Change Field (External Factors)

The 10th digit indicates state changes caused by external factors.

Example:

```
WARNING: -
Suncity HSG70 1000000002 0 HSG70  (SP_MONITOR: MonitorSubsys)
                          ⬆
```

This digit can have one of three values:

0 – Everything is fine.
1 – State changed from bad to good.
2 – State changed from good to bad.

The 11th Digit of the State Change Field (Logical Units)

The 11th digit reports state changes in logical units.

Example:

```
WARNING: -
Suncity HSG70 10000000002 HSG70  lun(d100:3) (SP_MONITOR: MonitorSubsys)
                          ⬆
```

This digit can have one of three values:

0 – Everything is fine.
1 – A LUN state changed from bad to good.
2 – A LUN state changed from good to bad.

The details about the failure of the LUN follow in parentheses, in the format:

virtual_disk:state

where *virtual_disk* is the unit number of the virtual disk and *state* is any of the following:

0 – Good.
1 – Reduced.
2 – Reconstructing.
3 – Failed.

In this example, logical unit D100 failed.

In most cases, the RaidManager sends at least two consecutive email messages. The first message is always in the form:

```
---------------
From RaidManager Tue Oct 6 16:09:37 1998
Date: Tue, 6 Oct 1998 16:09:37 -0500 (EST)
From: RaidManager

This is an automatic message from your StorageWorks
RAID Agent, steamd. The following message was just received.
Please check your syslog files and RAID box!
```

```
Hostname: Suncity

WARNING: - A RAID system change has been detected: Suncity HSG70 OVRL=1
(SP_MONITOR: MonitorSubsys)

End Of Automatic Message.
-------------
```

The text of the second message will be similar to the following (depending on the error):

```
---------
From RaidManager Tue Oct 6 16:09:37 1998
Date: Tue, 6 Oct 1998 16:09:37 -0500 (EST)
From: RaidManager

This is an automatic message from your StorageWorks
RAID Agent, steamd. The following message was just received.
Please check your syslog files and RAID box!

Hostname: Suncity

WARNING: - Suncity HSG70 12000000000 HSG70 disks(disk10200:1 disk10300:2)
(SP_MONITOR: MonitorSubsys)

End Of Automatic Message.
-------------
```

NOTE: This example shows that disk10200 went from bad to good, and disk10300 went from good to bad.

Chapter 5

Using Storage Windows

Why Use the Storage Window?

The Storage Window allows you to configure your storage subsystem. Use the Storage Window to do the following:

- Configure the properties of the controller, host ports, and cache
- Create:
  - Striped device group (RAID 0)
  - Mirrored device group (RAID 1)
  - Striped mirrored device group (RAID 0+1)
  - Striped parity device group (RAID 3/5)
  - Individual device (JBOD (Just a Bunch of Disks))
- View the status of virtual disks, communications LUN, and battery
- Update the controller firmware

Configuring a Controller

Your controller's operating parameters are stored under six tabs in the Controller Properties window, which you can access by one of two methods:

- Double clicking a controller icon  in the Storage Window
- Right clicking a controller icon in the Storage Window and selecting *Properties*.

A change in controller settings requires a controller restart for it to take effect. The program prompts you to confirm the restart.

Modifying the General Properties of the Controller

The properties of the top and bottom controllers, such as type, serial number, SCSI address, firmware revision, hardware revision, and common parameters are stored under the General tab.

To configure the general properties of the controller, click the General tab. Refer to Table 5–1 for a description of each general property.

Table 5–1 General Tab in the Controller Properties Window

What you can change	Description
Enable Command Console LUN alias	The Command Console LUN (CCL) appears as a virtual device to your host. If your host allows device aliases, you can assign an alias to the CCL. To use this feature, enable your CCL. Click the Enable box and enter a name in the text box. Ensure the format of the name follows the guidelines for your operating system.
Allocation class	Use extreme caution when changing the setting of this field. **CAUTION:** Changing the setting of the allocation class of your controller may cause data corruption and your host system may require restarting.
Enable autospare	If a replacement policy is in place and autospare is enabled, a failed drive will look for a spare drive. Check your legend for icons that show the status of this process. To determine whether a replacement policy is set, click the Settings tab in the Virtual Disk Properties window. Note that this option is not available on devices using RAID 0 or JBOD storage.
Time and date	The controller uses the internal clock to time stamp event logs and status messages. Both the time and date fields must have values to change either parameter. In other words, you cannot change or enter a time and leave the date field blank.

Table 5–1 General Tab in the Controller Properties Window (Continued)

What you can change	Description
Enable remote copy mode	Enable remote copy mode activates remote copy for a controller pair (subsystem). This feature requires you to first enable remote copy mode for the controller. To disable this feature, first remove all remote copy sets and remote copy set connections from the Connections tab of the Controller Properties window
Remote copy mode	The Remote copy mode field displays the name assigned to the controller pair when remote copy was enabled. To change the value for this field, you must first delete all existing remote copy connections from the Connections tab of the Controller Properties window.

Viewing the Properties of the Host Port

The Host Ports tab displays the following information:

- Port ID
- Fibre Channel profile
- Requested topology
- Actual topology
- Remote copy mode name that was assigned when remote copy was enabled

Modifying Properties of the Cache

The Cache tab provides the following information:

- Write cache size
- Cache version
- Cache status
- Unflushed data in cache
- Cache flush time (seconds)
- Cache uninterruptible power supply (UPS) settings
- Enables mirrored cache

Confirm the following:

- Cache flush_time: (seconds): is 10
- No UPS is selected

Viewing the Communications LUN

Click the Communications LUN tab to display the properties of the CCL. If the CCL (SWCC virtual LUN) is disabled, the options under this tab are unavailable. For more information about Floating and Fixed options and about the CCL, see Appendix A, Using the Command Console LUN.

Modifying the Connection Properties

Click the Connections tab to modify the connection properties, shown in Table 5–2.

Table 5–2 Connections Tab in the Controller Properties Window

What you can change	Description
Connection name	The connection name is a unique string of alphanumeric or punctuation characters that identifies a connection between a host bus adapter and the HSxxx controller. The host performs a Fibre Channel bus scan when it receives notification of a change to the fabric. As part of its device discovery process, the host then identifies the HSxxx as a SCSI device and login to the HSxxx controller. As the host performs the login, the HSxxx controller allocates an entry in the host connections table and assigns a connection name to the new connection. Subsequent logins by the host will use this same connection name and entry. Controller-produced connection names take the form "!NEWCONNnn", where nn is a two-character, decimal integer. This string format is not allowed for user-created connections.
Operating system	You can set your controller to operate with a variety of operating systems. Refer to the release notes for operating systems compatibility.
Unit offset	A decimal integer used to determine the LUN address of a virtual disk on a specific connection. Offsets can range from decimal 0-199.

Viewing Properties of the Battery

The Battery tab provides the following information:

- The state of the battery
- The expiration date of the battery

Creating Virtual Disks

You can use the Virtual Disk Wizard to create different types of logical storage units (called virtual disks) on your subsystem.

You can create the following types of virtual disks:

- Single-device virtual disks (JBODs)
- Striped virtual disks (RAID 0)
- Mirrored virtual disks (RAID 1)
- Striped mirrored virtual disks (RAID 0+1)
- Striped parity virtual disks with parity across all drives (RAID 3/5)

Note that the capacity of the smallest member, not the largest, determines the maximum capacity of RAID-based virtual disks.

- The maximum capacity of RAID 0 virtual disks is equal to the number of members times the capacity of the *smallest* member.
- The maximum capacity of RAID 1 virtual disks is equal to the capacity of the *smallest* member.
- The maximum capacity of RAID 0+1 virtual disks is equal to the number of members in one stripe times the capacity of the *smallest* mirrorset member.
- The maximum capacity of RAID 3/5 virtual disks is equal to the number of members minus one times the capacity of the *smallest* member.

Before you can create virtual disks from a physical device, your controller must know of the device. You can add devices online without restarting the controller.

In the following procedure, you add a physical device before you create a virtual disk.

To add a physical device and then create a virtual disk:

1. From the Navigation Window open a Storage Window within a desired subsystem.

2. Click *Storage* > *Add* in the Navigation Window.
3. If there is no user input in the Storage Window within an hour, you are prompted to enter a password. Type the SWCC password in the Security Check window and click *OK*.

   The SWCC password was created when you installed the Agent. To change the password, open the Agent Configuration utility on the agent system (host).
4. Select the type of virtual disk that you want to create, and click *Next* in the Add Virtual Disk Wizard – Step 1 of 5 window.
5. Select the physical devices to include in the virtual disk by clicking them in the Available Storage field in Add Virtual Disk Wizard – Step 2 of 5 window.

   As you click a physical device, it is added to the Selected Devices field. If you selected JBOD in the previous step, you can select only one device.
6. Click *Next*. You see the Add Virtual Disk Wizard – Step 3 of 5 window.
7. Type the capacity of the virtual disk in the Capacity for Virtual Disk field, and click *Next* in the Add Virtual Disk Wizard – Step 3 of 5 window. This window provides you with the maximum and minimum megabytes that you can choose for a capacity.
8. Type the unit number, operating parameters, and options for the virtual disk, then click *Next*. To save the controller configuration, select the *Save controller configuration to virtual disk setting* in the Add Virtual Disk Wizard – Step 4 of 5 window.
9. The Add Virtual Disk Wizard – Step 5 of 5 window – displays the selections that you made in steps 1-4.
10. If you are satisfied with your choices, click *Finish* to create the virtual disk.

IMPORTANT: The time required to initialize a virtual disk depends on the number of members and its size. During initialization, the virtual disk is unavailable for I/O. You should not use the virtual disks until initialization is complete.

Deleting Virtual Disks

The virtual disks in your subsystem are logical units that contain your user data. Although virtual disks do not exist in a physical sense, their logical structure ties together the physical pieces of your data spread across the members. Use extreme caution when deleting a virtual disk. You may delete valuable user data.

To delete a virtual disk:

1. Do one of the following:
   - ❏ From Windows NT 4.0, use Disk Administrator to delete the partition.
     OR
     From Windows 2000, use Disk Management to delete the partition.
   - ❏ From UNIX or OpenVMS, ensure that any file systems that were mounted on the device are unmounted and removed. If the drive was part of a logical volume, remove the device from the logical volume system.
2. Click the icon of the virtual disk that you want to delete.
3. Select *Storage* > *Virtual Disk* > *Delete* in the Storage Window.
4. If Client prompts you for your password, enter it.
5. When Client prompts to confirm the change, click *Yes* to continue. Client deletes your virtual disk from your configuration and refreshes the Storage Window.

Modifying Virtual Disks

You can modify the characteristics of your virtual disks in two ways:

- Change their operating characteristics
- Remove their members

CAUTION: Use extreme caution when modifying the characteristics of a virtual disk. You may be putting valuable user data at risk.

You can change the characteristics of a virtual disk by accessing its property sheets.

To access the property sheets of a virtual disk, refer to Table 5–3 and do one of the following:

- ❏ Double click the virtual disk icon  .
- ❏ Right click a virtual disk icon and select *Properties*.

Table 5–3 Virtual Disk Properties Window

Tab	Information
General	Lists the characteristics of the virtual disk.
Settings	You can change chunk size, reconstruction rate, replacement policy, and maximum cached transfer blocks. You can also enable or disable writeback cache by clicking the checkbox. Click the *OK* button to save the changes and to exit.
Membership	Displays the member devices. Can view a device by name and its current state, channel, target, and capacity.

Setting Passwords and Security Options (Network Only)

Password security prevents unauthorized users from changing or removing storage configurations. In SWCC, the following operations require a password:

- Changing controller configuration
- Changing virtual disk configuration
- Changing device settings

Security Options

There two security options, View Only and Make Changes. These are available from the Storage Window Options menu.

Password Security

Password security prevents unauthorized users from changing or removing storage configurations.

You create a password when you install the HS-Series Agent on a system. The password is encrypted and stored in the file where the Command Console Agent resides. To set or change a password, use the Agent Configuration menu.

Command Console allows a user with a valid password to make configuration changes for one hour. If an hour elapses without user input, the Command Console resets itself to View only. Any configuration change resets the timer and keeps the current password active for one hour.

Managing and Creating Spare Devices

Making a spare device part of a virtual disk protects the integrity of the RAID setup. A spare is especially important for virtual disks that have RAID requirements of two or more devices. If one device fails, the virtual disk instantly and automatically activates the spare device as a replacement.

A spare works as follows: if a device fails in a RAID 1, RAID 0+1, or RAID 3/5 virtual disk, the spare automatically replaces the failed device and the controller reconstructs all virtual disks of which the failed device was a member.

After the controller writes data to a spare, the spare becomes part of the same device group in which a device failed.

Creating a Spare Device

To create a spare device:

1. In the Storage Window, click the device that you want to use as a spare. For an automatic failed drive replacement, the device must be available and have a capacity equal to or greater than the lowest capacity drive in the group.
2. From the Storage menu, choose *Device*, then choose *Make Spare*.

Clearing Failed Devices

In the Storage Window, the icon of a failed device appears with an X covering it.

To clear the failed device:

1. From the Storage menu, select *Device.*
2. Then select *Delete*.

Using Configuration Files

You can use a configuration file to save a subsystem configuration and view or reconstruct it at another time. You can revert to a saved configuration at any time. Client reads the configuration file that you choose and sets up your subsystem accordingly.

Saving Configuration Settings to a File

To save the configuration settings for a subsystem:

1. Click *Storage* > *Controller Configuration* > *Save*.
2. Follow the instructions on the screen.

The current configuration settings, including caches, LUNs, host port, and stripe size, are saved to a file at the location that you specify.

Restoring Configuration Settings from a File

You can restore your entire subsystem from a saved configuration file. Client can restore your subsystem only if the configuration file corresponds to your subsystem's hardware configuration and if all of the controllers are attached to a serial connection.

CAUTION: Be aware of the configuration information in the configuration file that you choose. If you choose a file that is incompatible with the current configuration of data on your devices, you put your data at risk.

To restore your subsystem from a saved configuration file:

1. Select one of the displayed options:
   - ❏ If you need to reconfigure a failed controller that has existing virtual disks, select *Load configuration only*. The Client recreates your virtual disks, but it does not initialize them. Your data is not overwritten.
   - ❏ If you are configuring a new system, select *Load configuration and initialize virtual disks*.
2. Click *OK*.
3. When the Open dialog box displays, specify the location (path) and file name in the text box, then click *Open*. The configuration settings, such as caches, LUNs, host port, and stripe size are restored.

CAUTION: If the original hardware and connections are replaced or if the original configuration settings are not saved before making new changes, you cannot restore the original configuration settings.

Updating the Controller Firmware

For information and restrictions about downloading various versions of controller software, refer to the release notes for your version of Client. You can upgrade your firmware over a network or a SCSI connection.

1. Click *Storage* > *Update Controller Software* in the Storage Window. A window appears asking you to specify the firmware file that you want to load.
2. Type the name of the firmware file name (Its extension is *.fdi or .img*). Then click *Start Update*. When the firmware update is complete, the system automatically reboots and updates the controller firmware.

Understanding the Icons

You can obtain a definition of the icons by clicking *View* > *Legend* in the Storage Window.

The Storage Window provides detailed information in both physical and logical views of a subsystem in the Storage Window. In each view, icons represent device and virtual disk states. These icons change to indicate status. An X through a device indicates device failure. The Storage Window status bar indicates power, fan, temperature, and battery states.

Table 5–4 Description of Icons in the Storage Window Status Bar

Icon	Description
	Indicates that the cabinet fans are all operating normally
	Indicates a problem with the cabinet fans
	Indicates that the cabinet temperature is within its acceptable range
	Indicates that the cabinet temperature is out of its acceptable range
	Indicates that all power supplies are operating normally
	Indicates that the cache backup batteries are fully charged and operating normally
	Indicates a low charge condition on the cache backup batteries
	Indicates that the cache backup batteries have failed or are discharged

CLI Window

The CLI is a text-based interface utility for monitoring and configuring your storage subsystem. Because the configuration of the storage subsystem can be changed using CLI commands, we recommend that you allow CLI access only to users who are familiar with CLI operation.

The CLI Window, as shown in Figure 5–1 has a command-entry area and a command response area below it. You can enter commands in the command-entry area, and the controller responds with the results of the entry in the response area.

Accessing the CLI Window

There are two ways to access the CLI Window as follows:

From the Start menu:

1. Select *Command Console V2.4,* then select *CLI Window.*

From the Navigation Window:

1. In the Navigation Window, click the subsystem's host system icon to expand the tree and display the CLI Window icon.
2. Click the icon for the subsystem you wish to use with the CLI Window. The Navigation Tree expands the display to show the windows and pages available with this host system.
3. Click the CLI Window icon for your subsystem. If the program prompts you for your password, enter it and the CLI Window appears. Enter a CLI command in the command-entry area.

   NOTE: Controller utility programs should be run from the controller serial port and not from the Command Console Client CLI Window, as this will result in client and/or agent problems.

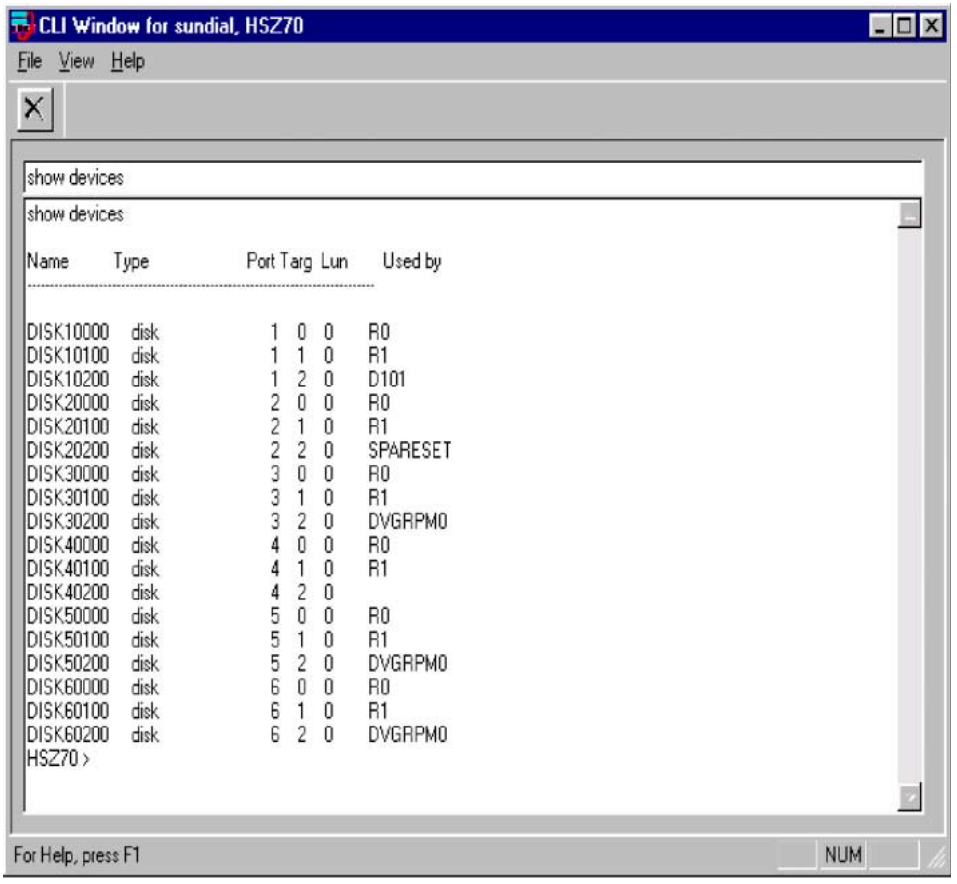


Figure 5–1. CLI Window

Chapter 6

Integrating SWCC with Compaq Insight Manager

You can use the HSGxx Storage Windows within Compaq Insight Manager version 4.23 or later. If your HSGxx controller uses Array Controller Software (ACS) version 8.5 or later, install the integration patch (HSG80 Shim). This patch allows you to use the HSGxx Storage Windows within Compaq Insight Manager to monitor and manage the controllers. HSG80 Storage Window version 2.4 is required to run the integration patch.

Installing the Integration Patch

To install the integration patch:

1. Verify that the HSGxx Storage Window for ACS 8.5 or later is installed by looking in Add/Remove Programs. (Click *Start* > *Settings* > *Control Panel* > *Add/Remove Programs).*
2. Verify that the HSG80 Storage Window version 2.4 is installed by looking in Add/Remove Programs *(StorageWorks HSG80 V2.4).*
3. Verify that Compaq Insight Manager version 4.23 or later is installed.
4. Install the integration patch from the Solution Software CD-ROM by double clicking *setup.exe* in the top-level directory. The SWCC Setup window appears.
5. Select HSG80 Controller Shim. If you do not have the HSG80 Storage Window version 2.4, also select HSG80 Controller.
6. Click *Next*.

The patch is installed in the same location as the original SWCC installation.

Integrating the HSGxx Storage Window with Compaq Insight Manager

You can open an HSGxx Storage Window from within the Windows-based Compaq Insight Manager 4.23.

To open an HSGxx Storage Window:

1. Look in Add/Remove Programs in the Control Panel to verify that the following are installed:
   - ❏ The HSGxx Storage Window for ACS 8.5 or later (required to open the correct Storage Window for your firmware).
   - ❏ The HSG80 Storage Window 2.4 *(StorageWorks HSG80 V2.4).* The integration patch uses files in this program.
   - ❏ Compaq Insight Manager 4.23 or later.
   - ❏ Compaq Insight Manager integration patch *(HSG80 Insight Manager Shim).*
2. Verify that you have installed the Compaq Insight Manager Agent and the StorageWorks Command Console HS-Series Agent on the same computer.
3. Add the name of the client system running Compaq Insight Manager to the Agent's list of client system entries and choose SNMP as a notification scheme.
4. Open Compaq Insight Manager.
5. To open the Server window, click the device that you want to observe in the Compaq Insight Manager Navigation window.
6. Click *Mass Storage* in the Server window. The Compaq Insight Manager Navigation Tree is displayed.
7. Click the + symbol next to *RAID Storage System.* The Navigation Tree expands to display the listing called *Storage System Information*.
8. Double click *Storage System Information*. You are given the status of the system.
9. Click *Launch*. The Storage Window appears.

Compaq Insight Manager Unable to Find the HSGxx Storage Window

If you install Compaq Insight Manager before you install SWCC, Compaq Insight Manager cannot find the HSGxx Storage Window.

To fix this, do the following:

1. Double click the Insight Agents icon *(Start > Settings > Control Panel).* A window appears showing you the active and inactive Agents under the Services tab.
2. Highlight the entry for Fibre Array Information and click *Add.* The Fibre Array Information entry is moved from Inactive Agents to Active Agents.

Removing the Integration Patch Disables Storage Window

If you remove the integration patch, HSG80 Storage Window version 2.4 cannot work. You have to reinstall HSG80 Storage Window version 2.4. The integration patch uses some of the same files as the HSG80 Storage Window version 2.4.

Chapter 7

Troubleshooting

Troubleshooting Connection Problems

SWCC is a TCP/IP socket-based application. As a result, SWCC requires that each node running a SWCC Client or Agent has access to a valid hosts file or Domain Name Service (DNS) server. Minimally, the valid hosts file must include the system itself and all systems running the SWCC Client and Agent.

DHCP and WINS

SWCC does not support the DHCP or the WINS; however, you can still use these protocols on systems that do not run the Command Console.

Before checking whether your system uses DHCP or WINS first verify that your network is running.

- For Windows NT or Windows 2000, run *netstat* at the command prompt on the Agent and check the active TCP/IP connections.
- For UNIX, run *netstat* with the correct options. Reference netstat main pages in UNIX help information.
- For other operating systems, refer to the operating system documentation.

To determine whether your system is using DHCP or WINS on Windows 2000 or Windows NT 4.0:

1. Right click Network Neighborhood on the desktop.
2. Select *Properties*.
3. Click the *Protocols* tab.

4. Select *TCP/IP*, then click *Properties*. The Microsoft TCP/IP Properties window appears.

"Access Denied" Message

This section describes some common reasons for a Client to receive an "Access Denied" message when it attempts to add an agent system to the Navigation Tree.

Aliases Not Checked

Ensure that the Agent's host system is configured to recognize the Client by its assigned name rather than by an alias. If the host system has been configured to recognize the Client by an alias, remove the alias from the system's hosts file.

When SWCC Agents scan the Client authorization list, they do not check aliases. SWCC will not scan the hosts alias list to verify if an alias matches the Client authorization list.

Entry in the Client Authorization List Does Not Match

You may see an "Access Denied" message if the name of the client system that you entered in the Agent configuration utility does not match the one for DNS or in the agent system's hosts file. The hosts file on Windows NT 4.0 and Windows 2000 is at *\winnt\system32\drivers\etc*.

Your system may be configured to do one the following:

- Check its local hosts file first, then go to DNS (most common setup for Windows NT and Windows 2000).
- Go to DNS first, then check its local hosts file.
- Ignore DNS even if configured.
- Ignore the local hosts file.

To determine your system configuration (Windows NT and Windows 2000):

1. Right click *Network Neighborhood* (on the desktop).
2. Select *Properties*.
3. Click the *Protocols* tab.
4. Select *TCP/IP*, then click *Properties*. The Microsoft TCP/IP Properties window appears.

5. Click the *WINS Address* tab. If your computer uses DNS, the Enable DNS for Windows resolution option is selected; you do not need to have Enable LMHOSTS Lookup selected.

   If WINS servers are available on the network, the *LMHOST* file can be used. SWCC does not support WINS.

6. To determine the IP address for the system, click the IP Address tab in the Microsoft TCP/IP Properties window.
7. To determine the full name of the system, click the DNS tab.

For other operating systems

Generally, the entry for an Agent in the Client authorization list must match what gethostbyaddr(<client IP address>) returns in the hosts agent h_name field if gethostbyaddr(<client IP address>) is executed on the Agent system. If the hosts files names on all systems are not identical, the h_name returned may vary on different Agent systems. For example,

xxx.xxx.xxx.xxx client.somewhere.com client

returns client.somewhere.com in the h_name field, but

xxx.xxx.xxx.xxx client client.somewhere.com

returns client in the h_name field.

The best way to determine what to use for a Client name in the Client authorization list is to write a program that runs on the Agent system and prints the h_name field returned by gethostbyaddr(<client IP address>).

Multiple Agents

If the Agent system is running multiple SWCC Agents (for example, to support different controller types), the client system must be authorized for all Agents. If the client system is missing from any authorized Client list of an Agent, that Agent cannot be added to the Navigation Tree.

Adding New System by Using Internet Protocol Address may Cause Client to Stop Responding

The SWCC Client may stop responding if you attempt to add a system by using the agent system's IP address rather than its node name. This occurs when the client system does not have a DNS server configured that knows the agent system, and the agent system is not included in the client system's hosts file. To correct this situation, add the agent system to the hosts file on the client system.

If you receive an "Invalid host" or "Host not known" message when you attempt to connect to an agent system, do not enter the IP address. Correct your DNS server configuration. If it is correct, confirm that the DNS server knows the agent system. If you are not using DNS, verify the agent system is in the client system's hosts file.

"No Agent Running" Message When Adding System to the Navigation Tree

While attempting to add a new system to the Navigation Tree, you may see the message "No Agent running on specified system." This message may appear for several reasons. The following are the most likely:

- The wrong system name was entered.
- The Agent was not installed on the entered system.
- The Agent was installed on a system that stopped functioning.
- Client and Agent port names and numbers in the services file may not match. This may occur if the default value for an SWCC port was already in use.
- The specific Client required to support an Agent is not installed. For example, if the Agent system has only a KZPCC Agent and the client system has only an HSZ22 Client, the "No Agent Running" message appears.

  To verify that there is Client support for an Agent, look at the following registry key:

  HKEY_LOCAL_MACHINE\Software\DigitalEquipmentCorporation\Command Console\AppletManager

  You should see a series of keys for supported products.
- Make sure the system names used for the Client and Agent match exactly. As a general rule, use lowercase letters when entering names.
- You entered the host name in the *\winnt\system32\drivers\etc\hosts* file. The host name is not required here, but TCP/IP looks at this file first to resolve a host name.

Troubleshooting the Client

Authorization Error When Adding an Agent System

If you receive an authorization error when you add an agent system to the Navigation Tree, your client system may be missing from the Agent's list of client system entries. If you have more than one type of Agent installed on that agent system, the name of your client system appears on each Agent's list of client system entries.

Cannot Open Storage Window

If you cannot open a Storage Window from the Navigation Tree or in stand-alone mode, the client system access option for the subsystem to which you want to connect is probably set to Overall Status (0), disabling access to the Storage Window.

Client Hangs When LUN Is Deleted

If you delete the LUN that is used by the communication drive, you cannot communicate with the controller. You must assign another LUN to the monitored subsystem before deleting the original LUN.

If you disable the Command Console LUN, the Client may lose its connection with the subsystem. If you need to disable the communications LUN, first assign another LUN as the communications LUN.

CLI RUN Commands

Do not issue RUN commands in the CLI window. Instead, issue RUN commands from a maintenance terminal connection.

Event Notification for Subsystems Connected to a Client System

To use the event notification features, an Agent must be installed and running. Create a local network connection by running Client and Agent on the same Windows NT/2000 host computer. Install each component as if Client were running on a remote system.

Invalid or Missing Fault Displays and Event Logs

Invalid or lost notifications may occur when the client system loses connection with a subsystem. The client system receives notification about most of the changing subsystem faults at monitored intervals. If the client system no longer receives notification about subsystem faults, then changes to that subsystem will not appear in the client system's Navigation Tree, Storage Window (if applicable), Fabric Window (if applicable), and Event Viewer.

For example, while client system's connection with a subsystem is broken, you will not receive event logs about that subsystem, except the lost connection notification.

The following list describes common causes for lost connections. After you fix the physical and/or software problem that is listed below, you need to close and reopen the Storage Window for that subsystem to get its latest status.

- RAS connections - Remote Access Service (RAS) connections are not full-time. If no RAS connection exists, events are not logged to the Event Viewer Application Log.
- Serial controller connections - There may be a bad or missing serial cable. To correct this situation, replace or plug in the cable.
- Network connections - Agent may be missing or not running.
- Network connections - There may be network discontinuity.
- The Agent may not be properly configured for a client system.
- If your setup includes a controller, the controller may have halted, reset, or hung. To repair the situation, restart or replace the controller.
- If your setup includes virtual disks, the virtual disk being used for communicating with the subsystem is no longer available.

Pager Notification Continues After Exiting the Command Console Client

You may have noticed continuous pager notification in response to subsystem faults, even though you have exited Command Console Client. This behavior is normal.

AES runs as a service under Windows NT and Windows 2000. It continues to run after you exit the Command Console Client. AES communicates with Agents and activates paging when a subsystem event occurs.

To stop pager notification, stop AES. For information about stopping AES, see About the Asynchronous Event Service.

Reconfiguration After Controller Replacement

If you replace a controller in your subsystem, you must reconfigure your Agent's storage list to match the new hardware.

Some Graphics Do Not Scale Well with Large Fonts

Display small fonts when using Client. Some graphics do not scale as well if large fonts are used.

Starting Client from the Command Prompt

To start the Client with network connections from the command prompt, enter the following at the command prompt on the client system:

```
\path_to_client_directory\swcc.exe -d your_host_system your_host_subsystem
```

where -d your_host_system your_host_subsystem is an optional set of parameters that enables you to specify a system and a subsystem to start Client.

For example:

```
C:\>\Program Files\Compaq\SWCC\swcc.exe -d hostsystem subsystem
```

If you specify these parameters when the Client opens, the system is selected and the subsystem is displayed in the Storage Window. If Client is not already aware of the system and the subsystem, it adds them to the Navigation Tree.

Warning Message Windows

You may see warning messages, such as "Command Execution Error" along with detailed information. These messages indicate problems with the controller, rather than with the software. The controller is responding to problems in parsing and executing commands from Client and Agent.

Virtual Disk Recovery from a Configuration File

If you delete a virtual disk, the member drives are all reinitialized and data is lost. You cannot restore a virtual disk's data by changing the configuration. A configuration file contains information only about the structure of a virtual disk. It does not store data.

Troubleshooting the HS-Series Agents

This section describes how to troubleshoot the HS-Series Agents.

Agent Sensitive to Alphanumeric Names

Agent may not accept some alphanumeric name forms, particularly those with embedded underscores. If you experience difficulties with a node name, change the node name to one that the Agent accepts.

HS-Series Agent Interaction

If an HSZ22 controller is connected to a system when the controller scans for subsystems, the HS-Series Agent (except for the HSZ22) for Tru64 UNIX and Windows NT will identify the HSZ22 controller as an HSZ20. The Agent scans for subsystems during installation and upon request.

There are two ways to correct this issue:

- Avoid the problem - Shut off the HSZ22 controller during the HS-Series Agent installation. After installation, turn on the HSZ22 controller and restart the system.
- Repair the problem - During installation of the HS-Series Agent, delete the erroneous entry. The HSZ22 entry appears on the second screen of the configuration utility. You can identify it by its serial number, firmware version, and by the drive used to access the subsystem.

HSZterm Utility Interaction Problems

If you use the HSZterm Utility (Set host/SCSI), do not use the same controller that SWCC is accessing. If you do, the connection will interfere with SWCC.

Invalid Cache Errors

Your controller module, cache module, and subsystem contain the configuration information that is used for synchronization. This configuration information is called metadata. The firmware reports an invalid cache error on an affected controller if there is a mismatch between the metadata in the controller module and a cache module containing unwritten data. This mismatch may result in the loss of the unwritten cache data if the error is not cleared properly.

You may lose valid data if you clear unwritten cache data. Client displays a message and prompt box when an invalid cache error occurs. Use the CLI window to clear unwritten cache data as the error is cleared. For information about how to clear unwritten cache data, see the "Invalid Cache Errors" topic in online Help.

Cluster Integration for the HS-Series Agents

This section describes how to integrate the SWCC with the Windows NT Server, Enterprise Edition (with Microsoft Cluster Server).

How to Integrate SWCC with Windows NT

Integrating SWCC with the Windows NT Server, Enterprise Edition (with Microsoft Cluster Server) allows you to configure and monitor a subsystem within the cluster environment. You need the following to perform cluster integration:

- A valid, working stable cluster
- An Agent installed on a disk that is on a non-shared SCSI bus
- An Agent on each cluster node of the cluster

To integrate a Windows NT cluster with SWCC:

1. Click *Settings* under the *Start* menu, then click *Control Panel*. Double click *Services*. The Services window appears.
2. Select *Steam* from the drop-down list for the Service field, and then click the *Stop* button. Steam, which stands for StorageWorks Enterprise Array Manager, is the name for the HS-Series Agent service. This action stops Steam, and its status no longer displays as Started in the Services window.
3. Click *Startup*. A smaller Services window appears.

4. Select *Manual*, and then click *OK* to disable the automatic start of the service. You are returned to the main Services window.
5. Click *Close* to exit the Services window.
6. Repeat steps 1-5 for each cluster node.
7. Click the *Cluster Administrator Utility* entry under the *Administrative Tools* group. The program's main screen appears.

   NOTE: Microsoft develops Cluster Administrator Utility. For further information about the software, see Microsoft's documentation.

To complete the Cluster Administrator Utility information:

1. Click your cluster group. The resources in your cluster group appear.
2. Verify that your cluster group includes the quorum disk.
3. Right click the cluster group. A drop-down menu appears.
4. Select *New*, then *Resource*. The New Resource window appears.
5. Type the SWCC Agent's name and description. Under Resource Type, select *Generic Service* from the drop-down menu. Under Group, select *Cluster Group*.
6. Click *Next*. The Possible Owners window appears.
7. In the Possible Owners field, select the nodes in your cluster where you want the SWCC Agent to run.
8. Click *Next*. The Dependencies window appears.
9. Select the following resources: Cluster IP Address, Cluster Name, and Quorum Disk.
10. Click *Add* to bring these resources online before starting the SWCC Agent.
11. Click *Next*. The Generic Service Parameters window appears.
12. Type Steam in the Service Name field. Leave the Start-up Parameters field empty.
13. Select *Use Network Name* for computer name.
14. Click *Next*. The Registry Replication window appears.
15. Click *Finish*. A message stating that you have successfully created a generic service resource appears.

Multiple Communication Lost Messages

On a client system, AES monitors every agent system that is included in the Client's Navigation Tree. If an Agent fails on a system that AES is monitoring, AES generates a page and an event log entry for the Agent at every polling interval indicating that communication has been lost. To stop the page and event log entries, remove the system entry in the Command Console's Navigation Tree.

Event Updates

You must manually update any node added to the Navigation Tree by using cluster alias and any Storage Window that opens off of that cluster alias. If you have a pager configured for automatic updating, you must add the individual nodes of the cluster to the Navigation Tree.

Multiple Pages

AES may send multiple pages if an Agent moves from a failing node to a working node. When the Agent fails over, a TCP/IP peer reset error may appear in the active Storage Window that had been connected to that Agent.

Appendix A

Using the Command Console LUN

This appendix explains how to avoid errors when configuring the CCL. Note that Windows NT and Windows 2000 with SCSI-2 do not support the CCL.

About the Command Console LUN (CCL)

The CCL is a preconfigured virtual LUN, located on controller A, LUN 0. LUNs identify different types of storagesets. The host uses LUNs to access the storageset.

Command Console sees the CCL as a virtual disk; however, the CCL cannot store information. The CCL is used only as a communication path between the controller and Command Console.

If you enable the CCL, the controller reserves one LUN address for Client or Agent use. The reserved LUN address is stored under the Communications LUN tab. The CCL does the following:

- Allows the host to recognize the RAID Array as soon as it is attached to the SCSI bus and configured on the operating system.
- Serves as a communications device for the HS-Series Agent. The CCL identifies itself to the host by a unique identification string. This string, HSG60CCL or HSG80CCL, is returned in response to the inquiry command.

The default state for the CCL is enabled. To determine the address of the CCL, enter the following command:

```
HSG60 > SHOW THIS_CONTROLLER
```

OR

```
HSG80 > SHOW THIS_CONTROLLER
```

Enabling and Disabling the CCL

Do not use your controller's CLI to disable the CCL while the Command Console is running. You may lose not only communication between the Client and the Agent, but also your data. Typically, the CCL remains enabled when you use Command Console. If the Agent system is running Windows NT or Windows 2000 with SCSI-2, disable the CCL and create a virtual disk before you run Command Console.

To disable the CCL, enter the following CLI command:

```
HSG60 > SET THIS_CONTROLLER NOCOMMAND_CONSOLE_LUN
```

OR

```
HSG80 > SET THIS_CONTROLLER NOCOMMAND_CONSOLE_LUN
```

To enable the CCL, enter the following CLI command:

```
HSG60 > SET THIS_CONTROLLER COMMAND_CONSOLE_LUN
```

OR

```
HSG80 > SET THIS_CONTROLLER COMMAND_CONSOLE_LUN
```

In dual-redundant controller configurations, these commands change the CCL setting on both controllers. The CCL is enabled only on host port 1. At least one storage device of any type must be configured on host port 2 before you install the Agent on a host connected to host port 2.

Select a storageset that is not likely to change and configure it. The Agent can use this storageset to communicate with the RAID Array. If you later delete this storageset (LUN), the connection between the Agent and the RAID Array is lost.

Using an Initial Configuration

Your storage subsystem may not be configured when you first install it so there may be no virtual disks for Command Console to use. You cannot configure virtual disks because you cannot establish a connection. The Command Console LUN allows you to establish the first connection.

Before you run Command Console, from the CLI window enable the CCL. Note that if you are using SWCC with a SCSI-2 connection with an Agent running on Windows NT or Windows 2000, you must disable the CCL and create a virtual disk.

Preserving Virtual Disk IDs

In some operating systems, you may disable the CCL to preserve virtual disk IDs. On Windows NT and Windows 2000 systems with SCSI-2, the LUN appears as a drive letter that you can use only for this purpose. In this case, you must use the controller's CLI window to configure at least one virtual disk for communication before you run Command Console.

Safely Disabling the CCL

To disable the CCL while the Command Console is connected, you need to have at least one virtual disk remaining on your subsystem. Then, exit Client and stop running the Agent. Disable the CCL from the CLI window. Reconfigure Agent and Client to use the remaining virtual disk for communications.

Setting the Fixed/Floating Option

In Command Console, if you select the Fixed option from the Add Virtual Disk wizard, the CCL remains assigned to that location. Client reserves the address of the LUN, and you cannot use the Add Virtual Disk wizard to create virtual disks.

CAUTION: The Fixed option works only with the Add Virtual Disk wizard. You can still overwrite a LUN address assigned to the communications LUN, from CLI window, even if the Fixed option is selected.

If you select the Floating option, you can use the LUN address currently assigned to the communications LUN to create a virtual disk. If you use this address, your controller automatically "floats" the CCL to another address and you lose communication with your subsystem.

To select the fixed/floating option:

1. In the Device window, double click the icon for your controller to display its property sheets. If you have a dual-redundant controller configuration, you can use the property sheets of either controller.
2. Click the Communications LUN tab. The operating parameters for the communications LUN are displayed.
3. Click either Floating or Fixed to select it.

NOTE: Changes to your controller configuration require password access. The program prompts you for the appropriate password on your first attempt to modify the controller.

Cautions When Using the CCL

Be aware of the following cautions when using the CCL:

- If you select Client's Floating option and use the CCL's address to create a virtual disk, you lose communication between Client and your Agent. You must reconfigure and restart your Agent to have it recognize either the new CCL address or an existing virtual disk that is used for communication.
- Within your controller, the CCL always floats to another LUN address if you attempt to use its address to create a virtual disk. The Client's Floating/Fixed option affects only the way the Client presents available LUNs to the Add Virtual Disk Wizard.
- Regardless of Client's Floating/Fixed option setting, if you restart your controller, its CCL becomes the lowest available LUN combination that is not already assigned to a virtual disk. If you delete a virtual disk with a LUN address lower than that of the CCL and then restart the controller, the CCL automatically moves to the lower address. The result is a loss of communication with your subsystem. You must reconfigure and restart your Agent to have it recognize either the new CCL address or the address of an existing virtual disk used for communication.

Appendix B

Interpreting SNMP Traps

This chapter describes the format of an SNMP trap. When a physical storage device, a logical storage unit, or a physical enclosure component changes state, the HS-Series Agent sends an SNMP trap to every system that the SNMP option is enabled. The trap appears appears in the Agent's list of client system entries.

An Agent SNMP trap consists of the following information fields:

- Source IP address
- GENERIC = 6 (6 = ENTERPRISE-SPECIFIC VALUE TO FOLLOW)
- SPECIFIC = 0 or 1, where:
  - "0" indicates that the storage component transitioned from a bad to a good state
  - "1" indicates that the storage component transitioned from a good to a bad state
- Object ID (OID) variable of the offending storage component
- OCTET STRING value returning the name of the subsystem containing the storage component specified by the OID Variable

Object ID (OID) Variables

Each OID is prefixed by a Base Enterprise Number (BEN) for the Command Console product. The default BEN for Command Console Agents is as follows:

1.3.6.1.4.1.36.2.15.21

(iso.org.dod.internet.private.enterprises.dec.ema.sysobjects.raidmanager)

The following are the OID values used by Command Console:

- Disk Status = BEN + .3.2.1.4

  (BEN + .subsys.ssStatusTable.ssEntry.ssDiskStatus)
- Power Supply Status = BEN + .3.2.1.5

  (BEN + .subsys.ssStatusTable.ssEntry.ssPowerStatus)
- Cooling Status = BEN + .3.2.1.6

  (BEN + .subsys.ssStatusTable.ssEntry.ssFanStatus)
- Cache Battery Charge Status = BEN + .3.2.1.7

  (BEN + .subsys.ssStatusTable.ssEntry.ssCacheBatteryStatus)
- OverTemperature Status = BEN + .3.2.1.8

  (BEN + .subsys.ssStatusTable.ssEntry.ssTemperatureStatus)
- Communication Status = BEN + .3.2.1.9

  (BEN + .subsys.ssStatusTable.ssEntry.ssCommStatus)
- EMU External Input Status = BEN + .3.2.1.10

  (BEN + .subsys.ssStatusTable.ssEntry.ssEmuExtInputStatus)
- THIS Controller Status = BEN + .3.2.1.12

  (BEN + .subsys.ssStatusTable.ssEntry.ssController1Status)
- OTHER Controller Status = BEN + .3.2.1.19

  (BEN + .subsys.ssStatusTable.ssEntry.ssController2Status)
- LUN Status = BEN + .3.2.1.27

  (BEN + .subsys.ssStatusTable.ssEntry.ssLUNStatus)

If your SNMP Management Utility has the Agent MIB compiled, the utility should display the character string values shown in parentheses above. Note that some OID values specified in the MIB are not used for SNMP traps.

Octet String Values

The octet string value attached to a trap takes the form:

subsystem_name controller_type ID:state

where *subsystem_name* is the name of the subsystem to which the trap applies
controller_type is the model number of the controller in the subsystem
ID is the identification of the storage component that caused the trap
state is the status of the storage component that caused the trap

NOTE: A storage component can be a physical storage device, a logical storage unit, or a physical enclosure component.

ID and State Values

The range of values in the ID and status value fields varies, depending upon the type of storage component causing a trap. Acceptable values for various component are as follows:

- For disk drives:

  disk_name:state

  where *disk_name* is the name of the disk drive in the subsystem and *state* is either of the following:

  1 – Drive went from bad to good.
  2 – Drive went from good to bad.

- For temperature sensors:

  cabinet_number:sensor_type:state

  where *cabinet_number* is the cabinet ID, from 0-3, in a BA370 enclosure
  sensor_type is the EMU sensor, sensor 1, or sensor 2 in a 2100 enclosure
  state is either of the following:

  1 – Temperature went from bad to good.
  2 – Temperature went from good to bad.

- For cabinet fans:

  cabinet_number:fan_position:state

  where *cabinet_number* is the cabinet ID, from 0-3, in a BA370 enclosure
  fan_position is the fan location, from 1-3
  state is either of the following:

  1 – Went from bad to good.
  2 – Fan went from good to bad.

- For power supplies:

  cabinet_number:pwr_position:state

where *cabinet_number* is the cabinet ID, from 0-3, in a BA370 enclosure
pwr_position is the power supply location, from 1-2
state is either of the following:

1 – Power supply went from bad to good.
2 – Power supply went from good to bad.
3 – Power supply not present.

- For batteries:

  controller_device_scsi_id:state

  where *controller_device_scsi_id* is the SCSI ID of the reporting controller on the ontroller's device bus and *state* is either of the following:

  Good – Battery is good.
  Low – Battery voltage is low.
  Fail – Battery has failed.

- For LUNs:

  virtual_disk_number:state

  where *virtual_disk_number* is the unit number of the virtual disk and *state* is either of the following:

  0 – Good.
  1 – Reduced.
  2 – Reconstructing.
  3 – Failed.

Trap Example

An example SNMP trap for subsystem "subsys1" with a failing power supply on an Agent at IP address "16.82.16.01" would contain the following information:

```
Source address = 16.82.16.01
GENERIC = 6
SPECIFIC = 1
OID Value = 1.3.6.1.4.1.36.2.15.21.3.2.1.5 (iso.org.dod.internet.private.enterprises.
dec.ema.sysobjects.raidmanager.subsys.ssStatusTable.ssEntry.ssPowerStatus)
OCTET STRING = subsys1 HSZ70 1:3:2

--
-- iso(1) org(3) dod(6) internet(1) private(4) enterprises(1) dec(36)
-- ema(2) sysobjids(15) raidmanager(21)
RAIDMANAGER-MIB DEFINITIONS::= BEGIN
```

```
imports
 enterprises
 FROM RFC1155-SMI
 OBJECT-TYPE
 FROM RFC-1212
 Displaystring
FROM RFC-1213;


dec             OBJECT IDENTIFIER ::= { enterprises 36 }
ema             OBJECT IDENTIFIER ::= { dec 2 }
sysobjids       OBJECT IDENTIFIER ::= { ema 15 }
raidmanager     OBJECT IDENTIFIER ::= { sysobjids 21 }


-- raidmanager MIB
agent           OBJECT IDENTIFIER ::= { raidmanager 1 }
workstation     OBJECT IDENTIFIER ::= { raidmanager 2 }
subsys          OBJECT IDENTIFIER ::= { raidmanager 3 }

--      Agent Information Group

agManufacturer OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
 "The name of the Enterprise Storage Manager Agent manufacturer."

  ::= { agent 1 }

agMajVersion OBJECT-TYPE
    SYNTAX  INTEGER
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "Enterprise Storage Manager Agent Major Version Number (e.g., 3 for 3.0)."\

   ::= { agent 2 }

agMinVersion OBJECT-TYPE
    SYNTAX  INTEGER
    ACCESS  read-only
```

```
    STATUS  mandatory
    DESCRIPTION   "Enterprise Storage Manager Agent Minor Version Number (e.g., 0 for 3.0)."

   ::= { agent 3 }

agHostName OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "The Host System Network Name where the agent resides."

    ::= { agent 4 }

agEnterprise OBJECT-TYPE
    SYNTAX  OBJECT IDENTIFIER
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "The Enterprise ID subtree for Enterprise Storage Manager Agent MIB is registered."

::= { agent 5 }

agDescription OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "The Enterprise Array Storage Agent description."

::= { agent 6 }


-- Workstation Group

wsCPU OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
   "The workstation CPU type (e.g., 80486)."

    ::= { workstation 1 }

wsComputerType OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
```

```
    DESCRIPTION
    "The workstation Computer type (e.g., PC/AT)."

    ::= { workstation 2 }

wsModel OBJECT-TYPE
    SYNTAX  INTEGER
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "The workstation model number."

    ::= { workstation 3 }

wsSubModel OBJECT-TYPE
    SYNTAX  INTEGER
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "The workstation submodel number."

    ::= { workstation 4 }

wsBiosVersion OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "The workstation BIOS Version."

    ::= { workstation 5 }

wsOS OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "The workstation operating system name (e.g., WINNT)."

    ::= { workstation 6 }

wsOSMajVersion OBJECT-TYPE
    SYNTAX  INTEGER
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "The workstation OS major version number  (e.g., 3 for WINNT 3.51)."

  ::= { workstation 7 }

wsOSMinVersion OBJECT-TYPE
    SYNTAX  INTEGER
```

```
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "The workstation OS minor version number (e.g., 51 for WINNT 3.51)."

    ::= { workstation 8 }

-- Subsystem Group

ssTotalSubSystems OBJECT-TYPE
    SYNTAX  INTEGER
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "The total number of subsystems presently serviced by this agent."

    ::= { subsys 1 }

-- Subsystem Status Group

ssStatusTable OBJECT-TYPE
    SYNTAX  SEQUENCE OF SsEntry
    ACCESS  not-accessible
    STATUS  mandatory
    DESCRIPTION
    "This table holds the status information for each subsystem."

   ::= { subsys 2 }

ssEntry OBJECT-TYPE
    SYNTAX  SsEntry
    ACCESS  not-accessible
    STATUS  mandatory
    DESCRIPTION
    "The subsystem information entry."
    INDEX   { ssEntryIndex }

    ::= { ssStatusTable 1 }
SsEntry ::=

  SEQUENCE{
ssEntryIndex
INTEGER,
ssSubsysName
DisplayString,
ssOverallStatus
INTEGER,
ssDiskStatus
INTEGER,
ssPowerStatus
```

INTEGER,
ssFanStatus
INTEGER,
ssCacheBatteryStatus
INTEGER,
ssTemperatureStatus
INTEGER,
ssCommStatus
INTEGER,
ssEmuExtInputStatus
INTEGER,
ssEmuPresent
INTEGER,
ssController1Status
INTEGER,
ssController1SerNum
DisplayString,
ssController1RDAC
INTEGER,
ssController1Type
DisplayString,
ssController1ProdID
DisplayString,
ssController1FwRev
DisplayString,
ssController1HwRev
DisplayString,
ssController2Status
INTEGER,
ssController2SerNum
DisplayString,
ssController2RDAC
INTEGER,
ssController2Type
DisplayString,
ssController2ProdID
DisplayString,
ssController2FwRev
DisplayString,
ssController2HwRev
DisplayString,
ssUpsStatus
INTEGER,
ssLunStatus

```
INTEGER
}

ssEntryIndex OBJECT-TYPE
  SYNTAX  INTEGER
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
  "The index into ssStatusTable .

::= { ssEntry 1 }

ssSubsysName OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "The local Subsystem Name."

    ::= { ssEntry 2 }

ssOverallStatus OBJECT-TYPE
        SYNTAX  INTEGER  {
                GREEN(0),
                YELLOW(1),
                RED(2)
            }
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "This variable reports the overall status of the subsystem.
      GREEN: Normal Operating Condition
      YELLOW: Warning Condition
      RED: Subsystem Communication Failure; No response to Agent requests."

    ::= { ssEntry 3 }

ssDiskStatus OBJECT-TYPE
         SYNTAX  INTEGER  {
                 ALL_OK(0),

AT_LEAST_1_FAILURE(1)
                 }
         ACCESS  read-only
         STATUS  mandatory
         DESCRIPTION
```

```
        "This variable reports the overall status for the
         physical devices in the subsystem."

    ::= { ssEntry 4 }

ssPowerStatus OBJECT-TYPE
            SYNTAX  INTEGER  {
                 ALL_OK(0),
                 AT_LEAST_1_FAILURE(1)
               }
        ACCESS  read-only
        STATUS  mandatory
        DESCRIPTION
        "This variable reports the status for the
         Power Supply system in the subsystem."

    ::= { ssEntry 5 }

ssFanStatus OBJECT-TYPE
        SYNTAX  INTEGER  {
                 ALL_OK(0),
                 AT_LEAST_1_FAILURE(1)
               }
    ACCESS  read-only
    STATUS  mandatory
      DESCRIPTION
     "This variable reports the status for the
      FAN system in the subsystem."

    ::= { ssEntry 6 }

ssCacheBatteryStatus OBJECT-TYPE
        SYNTAX  INTEGER  {
                 NORMAL_CHARGE(0),
                 LOW_CHARGE(1)
               }
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "This variable reports the status for the
     Cache Battery in the subsystem. This status object is currently
     non-functional but in place for future use."

      ::= { ssEntry 7 }

ssTemperatureStatus OBJECT-TYPE
     SYNTAX  INTEGER  {
                NORMAL(0),
                OVER_TEMP_CONDITION(1)
              }
```

```
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "This variable reports the status for the
     Temperature in the subsystem."

        ::= { ssEntry 8 }

ssCommStatus OBJECT-TYPE
     SYNTAX  INTEGER  {
                NORMAL(0),
                 COMMUNICATION_FAILURE(1)
               }
   ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "This variable reports the status for the
     communication to the Primary Controller."

    ::= { ssEntry 9 }

ssEmuExtInputStatus OBJECT-TYPE
       SYNTAX  INTEGER  {
                ALL_OK(0),
                AT_LEAST_1_FAILURE(1)
            }
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "This variable reports the status for the
     EMU external input."

    ::= { ssEntry 10 }

ssEmuPresent OBJECT-TYPE
        SYNTAX  INTEGER  {
                EMU_NOT_PRESENT(0),
                EMU_PRESENT(1)
            }
     ACCESS  read-only
     STATUS  mandatory
     DESCRIPTION
     "This variable reports the availability of the
      Environment Monitoring Unit for the subsystem."

    ::= { ssEntry 11 }

ssController1Status OBJECT-TYPE
         SYNTAX  INTEGER  {
                  NORMAL(0),
```

```
                    FAILED(1)
                }
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "This variable reports the status for the
     Primary Controller."

    ::= { ssEntry 12 }

ssController1SerNum OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
   "The Primary Controller's Serial Number."

    ::= { ssEntry 13 }

ssController1RDAC OBJECT-TYPE
     SYNTAX  INTEGER  {
          SINGLE_MODE(0),
          DUAL_MODE(1)
              }
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "The Primary Controller MODE."

    ::= { ssEntry 14 }

ssController1Type OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "The Primary Controller's Type indicator."

     ::= { ssEntry 15 }

ssController1ProdID OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "The Primary Controller's Product ID."

     ::= { ssEntry 16 }

ssController1FwRev OBJECT-TYPE
    SYNTAX  DisplayString
```

```
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "The Primary Controller's Firmware Revision."

     ::= { ssEntry 17 }

ssController1HwRev OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "The Primary Controller's Hardware Revision."

     ::= { ssEntry 18 }

ssController2Status OBJECT-TYPE
     SYNTAX  INTEGER  {
                NORMAL(0),
                FAILED(1)
             }
   ACCESS  read-only
     STATUS  mandatory
   DESCRIPTION
   "This variable reports the status for the
    Secondary Controller."

   ::= { ssEntry 19 }

ssController2SerNum OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The Secondary Controller's Serial Number."

    ::= { ssEntry 20 }

ssController2RDAC OBJECT-TYPE
    SYNTAX  INTEGER  {
                    SINGLE_MODE(0),
                    DUAL_MODE(1)
                }
    ACCESS  read-only
    STATUS  mandatory
```

```
    DESCRIPTION
    "The Secondary Controller MODE."

    ::= { ssEntry 21 }

ssController2Type OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "The Secondary Controller's Type indicator."

    ::= { ssEntry 22 }

ssController2ProdID OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "The Secondary Controller's Product ID."

    ::= { ssEntry 23 }

ssController2FwRev OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The Secondary Controller's Firmware Revision."

     ::= { ssEntry 24 }

     ssController2HwRev OBJECT-TYPE
         SYNTAX  DisplayString
         ACCESS  read-only
         STATUS  mandatory
         DESCRIPTION
     "The Secondary Controller's Hardware Revision."

    ::= { ssEntry 25 }

ssUpsStatus OBJECT-TYPE
     SYNTAX  INTEGER  {
                    UPS_NOT_PRESENT(0),
                UPS_PRESENT(1)
            }

     ACCESS  read-only
      STATUS  mandatory
```

```
      DESCRIPTION
      "Uninterruptable Power Supply status (Currently for future use)."

    ::= { ssEntry 26 }

ssLunStatus OBJECT-TYPE
     SYNTAX  INTEGER  {
                  UPS_NOT_PRESENT(0),
                  UPS_PRESENT(1)
                }
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
    "LUN status."

  ::= { ssEntry 27 }

END
```

Glossary

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

Glossary Term	Glossary Definition
adapter	A device that converts the protocol and hardware interface of one bus type into that of another without changing the functionality of the bus.
Agent (HS-Series Agent)	Command Console's secure TCP/IP network communication program. Agent runs on your subsystems' host computer. It is available on several operating systems. One or more Client programs can access the HS-Series Agent running on a host system. Using the system's SCSI or Fibre Channel bus, the Agent can communicate with multiple subsystems on the same host system. You can configure the HS-Series Agent with password protection to prevent unauthorized users from accessing your subsystems. Collects data from the devices connected to the HS-Series controller and sends them to the Client. Enables the Client to communicate with storage connected to the HSxxx controller.
Allocation Class	A number that uniquely identifies a controller or group of controllers in a cluster. The allocation class provides a way of grouping disk-based virtual disks across controllers and distinguishing identical virtual disk names within the cluster. Legal values are 0-65535. The allocation class attribute applies to both controllers in a dual-redundant configuration.
array controller	A hardware and software device that provide communication between a system and one or more devices in an array.

Asynchronous Event Service (AES)	AES, which runs as a service in the background, collects and passes all traps from the subsystems to the appropriate Navigation Trees and individual pagers. AES needs to be running for Client to receive updates.
available	A state in which a device is operational but not yet in use as a member of a virtual disk.
bad block replacement (BBR)	Substitution of defect-free device blocks for defective ones. The procedure used to locate a replacement block, mark a bad block as replaced, and move data from the bad block to the replacement block. In some controllers this process occurs automatically.
block	Consecutive bytes of data stored on a storage device. In most subsystems, a block is the same size as a physical disk sector.
blower	An airflow device mounted in a device or controller shelf.
cache	A fast temporary storage buffer in a controller or computer.
capacity	The total amount of data that a physical or virtual disk can store.
channel	A SCSI device bus. Narrow SCSI device buses support up to 7 devices, and wide buses support up to 15 devices. Also called a “port.”
chunk	HS-series controller term for strip.
chunk size	HS-series controller term for strip size.
Client	The Command Console uses its associate program -- Agent -- for network connections to multiple subsystems. Client can use either a serial maintenance port or a host SCSI bus connection to connect to a single subsystem. From Client, you can view multiple storage systems and set up pager notification.
client list	List of Client nodes that are allowed to connect to an Agent over the network. The list is maintained in the *client.ini* file on the host where the Agent is installed. A client list entry includes the TCP/IP address or network name and the allowed access level for the host's subsystems of each Client.
client system	Computer on which the Client software is installed.
cold swap	Device replacement requiring that you power off the controller and cabinet shelves. This method is used if conditions preclude using the warm swap or hot swap method.
Command Console Client	Provides event notification and the Navigation Window.
configuration file	A file in which configuration information for a subsystem is stored. The file can be used to automatically configure the subsystem.

container HS-series controller term for a device group.

controller A firmware-driven hardware device used for communication between a host and storage devices. A controller translates bus protocols and hardware interfaces and adds functionality to the subsystem. Some controllers provide additional functionality by mapping storage devices to host-addressable, virtual disks with specific performance and availability features that use RAID techniques.

controller shelf A shelf designed to contain controller and cache memory modules. A controller shelf can contain two controllers in a dual-redundant configuration.

copy speed For HS-series controllers, the rate at which the controller writes mirrored data in a mirrored virtual disk. There are two speeds:

- Normal -- uses relatively few controller resources to perform the copy and has little impact on controller performance.
- Fast -- uses more controller resources, which reduces the time it takes to complete the copy, but also reduces overall controller performance.

device In its physical form, a magnetic or optical disk, tape, or CD-ROM that can be attached to a SCSI bus. A device provides large amounts of addressable storage to a host.

This term also means a physical device that is part of a controller's configuration. That is, it is known to the controller. After a device is made known to the controller, you can create virtual disks from it.

device driver A program that processes I/O requests for a particular type of device.

device group A logical, internal controller structure representing one or more devices that are linked as a group. Some controllers require that you must create device groups before you can create a virtual disk from them. Device groups are also known as containers. There are different types of device groups:

- Single-device virtual disks (JBODs)
- Striped virtual disks (RAID 0)
- Mirrored virtual disks (RAID 1)
- Striped mirrored virtual disks (RAID 0+1)
- Striped parity virtual disks with parity across all drives (RAID 3/5)
- Striped parity virtual disks with floating parity disk (RAID 5)

disk A storage device that uses rotating magnetic media to store data.

disk array	A collection of disk devices that are physically connected in an ordered structure.
dual-redundant configuration	For HS-series controllers, a configuration consisting of a primary and backup controller in one controller shelf. If the primary controller fails, the backup controller assumes control of the failing controller's devices.
environmental monitoring unit (EMU)	Some subsystem enclosures include an environmental monitoring unit that provides increased protection against catastrophic faults. The EMU works with the controller to warn about impending subsystem failures. The EMU senses such conditions as failed power supplies, failed blowers, elevated temperatures, and external air sense faults.
failed	A device state indicating that a device is inoperable and unavailable for use in a virtual disk. In some controllers, you can force a failed state, for instance to remove the device from the storage enclosure. In others, a device is marked as failed if you remove it as a member of a virtual disk.
failover	For HS-Series controllers, the process that takes place when one controller in a dual-redundant configuration fails and the other controller takes over. The other controller continues to direct the subsystem until the failed controller is again operational or is replaced.
good	A device state that indicates that a device is operational and in use by a virtual disk.
host	The primary or controlling computer to which a subsystem is attached.
host access ID	The target ID of the host computer allows exclusive access to a particular virtual disk. A virtual disk can be set to allow all or only one host target ID access to it.
host adapter	A device connecting a host system to a SCSI bus. Typically, the host adapter performs the functions of the lowest layers of the SCSI protocol. This function may be logically and physically integrated into the host system.
host functionality	You can configure your controller's host port targets for optimum performance and compatibility.
hot disks	Hot disks occur if the workload is poorly distributed across storage devices. A hot disk is a device with multiple hot spots. On a hot disk, host I/O requests begin to back up because of the concentrated request load. Hot disks cause subsystem performance to suffer.

hot spare
In a virtual disk, a device configured to automatically replace a failed device. If a virtual disk member fails, the controller automatically replaces the member with the spare device, and it rebuilds the member's data from the remaining devices in the virtual disk.

hot spots
Hot spots occur if the workload is poorly distributed across storage devices. A hot spot is a file or a group of files located on the same device that receive a very high concentration of I/O requests.

hot swap
A method of device replacement in which the system remains operational during device removal and reinstallation. The device being removed or reinstalled is the only device that is not operational during the process.

HSxxx Client
Provides the HSxxx Storage Window for storage connected to the HSxxx controller.

initialization
For subsystems, the process of restarting the controllers and reestablishing the subsystem's configuration and operation; that is, bootstrapping the subsystem. For virtual disks, the process of writing the controller's file structure to the virtual disk member devices. On the member disks, the file structure is represented by metadata.

JBOD (Just a Bunch of Disks)
JBOD is an industry term for a single-device virtual disk. A JBOD virtual disk does not provide any level of data redundancy.

known client list
See client list.

local area network (LAN)
A network that is confined to a single geographic location.

local connection
A direct hardware connection from Client to a single subsystem using either of two methods:

- A connection from a standalone computer running Client to the serial maintenance port on the controller
- A connection from a host system running Client to a subsystem on the host's SCSI bus

A local connection enables you to connect Client to one subsystem controller within the physical range of the serial or host SCSI cable.

logical drive
See virtual disk

logical storage unit
See virtual disk

logical unit number (LUN)
A SCSI bus supports a number of target devices, each of which has a number of logical units. A logical unit number is a logical unit's address on a target. A controller maps one or more SCSI logical units to a virtual disk that the host can access. The term "LUN" is also used to refer to the virtual disk itself.

mapping
The internal controller process of organizing single or grouped devices into virtual storage units (that is, virtual disks).

maximum block transfer
For HS-series controllers, the virtual disk parameter that specifies the maximum number of data blocks to be cached before writing data to virtual disk members. A data transfer greater than this size is not cached and is written immediately to disk. Valid values are 1-1024 (blocks).

member
Any device used in a virtual disk based on multiple devices. Any device in the device group on which the virtual disk is based.

metadata
Special data written to a device for the purpose of controller administration. Metadata improves error detection and media defect management for a device. It is also used to define device and virtual disk configuration.

mirrored cache
Some controllers offer high-performance cache hardware that can be set to operate in mirrored mode. In this mode, the cache data is duplicated and stored in cache memory in physically separate locations. If one copy of the data becomes corrupted or unavailable for some reason, the other copy is available for use.

A mirrored cache configuration provides complete protection for cached data. However, the cache memory effectively contains twice as much data for each host request, so the effective size of the cache is cut in half.

mirrored virtual disk
A group of storage devices organized as duplicate copies of each other. Mirrored virtual disks provide the highest level of data availability at the highest cost. Another name for RAID 1.

mirroring
The simplest form of data redundancy. Two or more devices form a mirrored device group. Each device is an exact copy of the other.

For read requests, data can be read from either device therefore increasing the throughput. Both devices can handle different requests simultaneously.

For write requests, data is written to both devices. If one device fails, all reads/writes are executed on the mirrored device group's other device. Therefore, mirroring provides excellent availability (unless the second device fails before the first (failing) device can be repaired or replaced).

Sometimes called shadowing.

The mirroring technique can also be applied to cache memory.

Navigation Tree — Provides access to the HSxxx Storage Window

Displays the status of your systems. It shows your systems in a hierarchical order.

Navigation Window — It contains the Navigation Tree and the menu options for configuring pager notification and the Navigation Tree.

network connection — A remote connection from Client to multiple subsystems using Agent over a TCP/IP-compatible network. Network connections enable you to concurrently monitor thousands of subsystems over a LAN or WAN anywhere in the world.

nonredundant — For HS-series controllers, a single-controller configuration.

The term is also sometimes used to refer to a RAID level that does not provide fault tolerance (for example, RAID 0).

normal — In mirrored virtual disks, a member state that indicates that a member contains exactly the same data as the other members do

parameter — A setting or value that defines a particular operating characteristic of a device, virtual disk, controller, or subsystem.

parity — Binary value calculated from user data used to detect if associated data becomes corrupt. Parity can also be used to correct corrupted data. Striped parity virtual disks use parity to improve data availability.

parity check — A virtual disk state that indicates that the controller is checking the integrity of a virtual disk's data.

partition — A logical division of a virtual disk, represented itself as a virtual disk to the host. Command Console enables the creation of virtual device partitions, but they are transparent to the user.

password — A code string used by Client with network connections to restrict configuration functions to privileged users. Passwords are set at the Agent at each host.

pedestal — A desk-side, floor-standing, storage enclosure capable of housing one or more controllers and associated devices to make up a complete subsystem.

physical device — A storage component installed in a subsystem.

physical disk — A storage component with rotating magnetic media that is installed in a subsystem.

port

The hardware and software used to connect a host controller to a communications bus, such as a SCSI bus or serial bus. On the device side of the controller, a port is called a channel. The term is sometimes also used to refer to the logical TCP/IP port that is used to access the Agent over the network.

port/target/LUN (PTL)

For HS-series controllers, the complete address of a physical disk on a device bus from which the controller derives the device name. The name, "disk11300", for instance, indicates a physical device at port 1, target 13, and LUN 00.

RAID (Redundant Array of Independent Disks)

RAID is an industry-standard set of techniques for configuring an array of storage devices into host-accessible, virtual disks with various cost, availability, and performance options.

Some common RAID levels are RAID 0, RAID 1, RAID 0+1, RAID 3, RAID 3/5,and RAID 5.

RAID 0

RAID 0 is the industry-standard name for disk striping. A RAID 0 virtual disk is also called a striped virtual disk.

In a RAID 0 virtual disk, host data is divided into strips spread in a stripe across virtual disk member devices. This technique provides much faster read and write performance than does reading and writing to a single device. A three-device, RAID 0 virtual disk has potentially three times the bandwidth of a single device because three separate small pieces of host data move in parallel.

RAID 0 is the only RAID level that does not provide some level of data redundancy. Because more devices can potentially fail and because there is no way to recover data for a failed device, RAID 0 virtual disks have less availability than equivalent-sized single disks.

RAID 0+1

RAID 0+1 combines the striping of RAID 0 and the mirroring of RAID 1 to provide the best combination of high performance and high availability. A RAID 0+1 virtual disk is also known as a striped mirrored virtual disk.

In a RAID 0+1 virtual disk, each RAID 0 stripe is mirrored to one or more duplicate device sets. This technique allows much faster read and write performance than does reading and writing to a single device. A six-device, RAID 0+1 virtual disk has potentially three times the bandwidth of a single device because three separate, small pieces of host data move in parallel.

In addition, the data is completely mirrored to one or more device sets so there is complete data redundancy for very high availability.

A RAID 0+1 virtual disk offers the highest performance and the highest availability of any RAID virtual disk type, but its cost is high. Such a configuration requires at least twice the number of devices that a RAID 0 configuration requires.

RAID 1

RAID 1 is the industry-standard term for device mirroring. A RAID 1 virtual disk is also called a mirrored virtual disk.

In a RAID 1 virtual disk, host data is written as a single large block to one device and the data is mirrored to one or more duplicate disks.

A RAID 1 virtual disk provides very high availability because the data is completely mirrored to one or more devices. Its performance is no better than that of a single device, however, because the data is transferred as one large block to and from these devices.

RAID 3

RAID 3 virtual disks use parity for data redundancy. A RAID 3 virtual disk is a type of striped parity virtual disk.

In a RAID 0 virtual disk, host data is divided into strips spread in a stripe across virtual disk member devices. An additional strip for parity information is appended to each stripe. This technique allows much faster read and write performance than does reading and writing to a single device. A three-device, RAID 3 virtual disk has potentially three times the bandwidth of a single device because three separate, small pieces of host data move in parallel.

In addition, because each data stripe is protected by parity information, there is a significant level of data redundancy for high availability. Some RAID 3 configurations use a dedicated parity device, but most controllers intersperse the parity strips within the data strips to maximize the read performance.

RAID 3 virtual disks provide high performance and high availability at reasonable cost. They are optimal for use in applications requiring relatively high data transfer rates and having relatively low I/O request rates.

RAID 3/5

RAID 3/5 sets are enhanced stripesets – they use striping to increase I/O performance and distributed-parity data to ensure data availability.

RAID 3/5 sets are similar to stripesets in that the I/O requests are broken into smaller “chunks” and striped across the disk drives. RAID sets also create chunks of parity data and stripe them across all members of the RAIDset. This parity data is derived mathematically from the I/O data and enables the controller to reconstruct the I/O data if a single disk drive fails. Thus, it becomes possible to lose a disk drive without losing its data it contained. Data can be lost, however, if a second disk drive fails before the controller replaces the first failed disk drive and reconstructs the data.

RAID 5

RAID 5 virtual disks use parity for data redundancy. A RAID 5 virtual disk is a type of striped parity virtual disk.

In a RAID 5 virtual disk, host data is written in its entirety as a strip representing one I/O request into a much larger stripe of I/O requests stored across the virtual disk membership. An additional strip for parity information is written into each stripe. This technique offers the same read performance as reading from a single device. However, in a RAID 5 virtual disk, multiple read I/O requests can occur resulting in a very high overall subsystem read performance.

Write performance, however, is much worse. Because writing a small strip of data into a larger amount of data on a device is really a read-modify-write operation, writing becomes time-consuming. In addition, because each data stripe is protected by parity information, there is a significant level of data redundancy for high availability.

RAID 5 virtual disks provide high read performance and high availability at reasonable cost. They are optimal for use in applications that have relatively high I/O read request rates and require relatively low data transfer rates.

read cache

A block of high-speed memory used to buffer data being read from storage devices by a host. A read cache responds to host read requests from local cache memory if possible rather than from external storage devices. Therefore, it increases the controller's effective device access speed.

The controller maintains copies of data recently requested by the host in cache, and it may fetch blocks of data ahead of a request in anticipation that the controller will access the next sequential blocks. In a typical read cache, host write requests are handled without involving caching.

read source

For HS-series controllers, a mirrored virtual disk option that controls the way data is read from the virtual disk's members. There are two Read Source options:

- Least Busy (default) -- the Normal, virtual disk member with the smallest I/O load is the target of all read operations.
- Round Robin -- each Normal, virtual disk member is the target of a read operation in sequential membership order. No preference is given to any member.

rebuild rate
The rate at which the controller reconstructs a failed device on a spare. To devote more or fewer cycles to rebuilding a failed device on a spare, adjust the rate using a scale from 1-100. A rebuild rate of 100 rebuilds the device at the fastest rate possible.

reconstructing
A physical device state that indicates that the controller is regenerating a failed device's data onto a replacement device that is part of a redundant virtual disk.

All user data remains available during the reconstruction process, but some performance reduction occurs if a request requires access to a device while it is being reconstructed.

reconstruction
Process of regenerating all of a failed member's data, writing it to a spare device, and incorporating the spare device as a redundant RAID virtual disk member.

All user data remains available during the reconstruction process, but some performance reduction occurs if a request requires access to a device while it is being reconstructed.

reconstruction rate
The speed at which a failed member's data is regenerated. The rate is adjustable. See rebuild rate.

reduced
A virtual disk state that indicates that a member device is missing, failed, or physically removed from a virtual disk.

redundant RAID
Any RAID level that uses redundant information to provide some level of data protection. RAID 1 (mirroring), RAID 0+1 (striped mirroring), RAID 3 (striped parity), RAID 5 (striped parity), and RAID 3/5 (striped parity) virtual disks are all examples of virtual disks that use redundant-RAID techniques.

regeneration

The process of recreating all or a portion of the data from a failed device using the surviving data and parity from the other virtual disk members.

In most controllers, data from all members remains available during regeneration, and the user is unaware that regeneration is occurring, except for a slight reduction in performance.

Regeneration of an entire disk member is called reconstruction.

Data regeneration occurs under one of the following conditions:

- The controller detects a hard read error on a virtual disk member. In this case, the controller transparently corrects the data and continues the read operation.
- The controller detects that a virtual disk member failed. In this case, the controller completely reconstructs the failed member.

SCSI (Small Computer System Interface)

An industry-standard parallel bus used to interconnect systems and physical devices.

SCSI device

A computer, a host adapter, a peripheral controller, or any storage element that can be attached to a SCSI bus.

SCSI ID

See target ID.

shadowing

See mirroring.

spare

A device state indicting that a device is designated as a hot spare for a failed device within a redundant RAID virtual disk. If a virtual disk member fails, the controller automatically replaces it with a spare device from the pool of spare devices.

The term is also used to refer to a spare device itself.

storageset

HS-series controller term for device group.

Storage Window

The Storage Window is a Client component that provides a graphical interface for configuring and monitoring to a selected subsystem.

strip

A RAID virtual disk using striping stores host data in pieces called strips. One strip is stored on each member device in the virtual disk. Together, the strips make up a stripe.

In some controllers, the strip size is used to tune the striped virtual disk for a specific application:

- If a virtual disk uses a small strip size compared to the size of the average host request, the controller can break the host data up into strips and can perform device accesses in parallel using RAID 3 techniques. This optimizes the virtual disk for applications requiring high data transfer rates.
- If a virtual disk uses a large strip size compared to the size of the average host request, the controller can use RAID 5 techniques to perform multiple read accesses in parallel on any device. This optimizes the virtual disk for applications requiring high I/O request rates.

Also called a chunk, segment, or stripe element.

stripe

A RAID virtual disk using striping stores host data in pieces called strips. One strip is stored on each member device in the virtual disk. Together, the strips across the member devices form a stripe.

strip size

The number of blocks of data that make up a strip.

In some controllers offering multiple-RAID-level virtual disks such as RAID 3/5, the relationship between the strip size and the average host I/O request size determines how the controller accesses the devices in the virtual disk and affects the request and data transfer performance of the subsystem.

striped virtual disk

Another name for a RAID 0 virtual disk.

striped mirrored virtual disk

Another name for a RAID 0+1 virtual disk.

striped parity virtual disk

Another name for a RAID 3, or RAID 3/5 virtual disk.

striping

A RAID technique in which host data is stored in pieces called strips. One strip is stored on each member device in the virtual disk. Together, the strips across the member devices form a stripe.

subsystem for the HSxxx controller

A controller and an array of physical devices attached to a host.

supported device

A device tested as functionally compatible with a controller in an approved hardware and software configuration.

surviving controller

The controller in a dual-redundant pair of HS-series controllers that assumes service to its companion's devices when the companion controller fails.

target A SCSI bus device. When one device addresses another device on a SCSI bus, it uses the target device's target ID to uniquely identify it.

target ID The physical address a bus initiator uses to connect with a bus target. Each bus target is assigned a unique target address. Also used to refer to a SCSI device ID itself.

TCP/IP An acronym for Transmission Control Protocol/Internet Protocol. This popular Internet network protocol uses IP addressing, where each network node has a unique network address. Client uses the TCP/IP to communicate with Agent.

transfer rate Date transfer speed over a SCSI bus. The transfer rate depends on the bus speed and width. Transfer rates are usually expressed in units of megabytes per second.

Some controllers allow you to set the maximum transfer rate on either their host or device bus. This feature allows you to limit the rate in special situations, such as those that require long bus cabling.

unit See virtual disk.

volume See virtual disk.

volume set See virtual disk.

virtual disk A series of physical drives linked together so that the software interprets the drives as being a single device. Logical storage units are called virtual disks and are accessible by the host. Each virtual disk has its own user-configurable parameters.

Some controllers use RAID techniques to provide virtual disks with various cost, availability, and performance options.

Also called logical drives, volumes, volume sets, logical storage units, logical units, units, and LUNs.

warm swap In some controllers, a feature that allows devices to be added, removed, or replaced while the subsystem remains operational, but with all activity on the controller's device buses stopped.

wide area network (WAN) A network that spans a large geographic area.

write-back cache

A cache configuration that increases the performance of host write requests. If a host requests a write operation, the controller writes the host's data first to the cache memory, completing the request quickly. It performs the slower operation of flushing data to the external storage device at a later time. The host sees the write operation as complete when the data reaches the cache.

For most controllers using write-back cache, the cache also increases performance with read cache techniques.

write only

A device state that indicates that while a member was being reconstructed an error was found on another member of the virtual disk.

write-through cache

A technique for handling host write requests in read caches. If the host requests a write operation, the controller writes data directly to the external storage device and updates the cache memory to ensure that the memory does not contain obsolete data. This technique increases the chances that future host read requests can be filled from the cache. The host sees the write operation as complete only after the external storage device is updated.

For some controller fault conditions, write-back cache resorts to write-through cache operation to protect your data.

Index

S

T

U

V

W