COMPAQ
STORAGEWORKS

Data Replication Manager HSG80 ACS Version 8.4P

Operations Guide

First Edition (April 1999)
EK-HSG84-DT. A01 / 128519-001
Compaq Computer Corporation

While Compaq Computer Corporation believes the information included in this manual is correct as of the date of publication, it is subject to change without notice. Compaq makes no representations that the interconnection of its products in the manner described in this document will not infringe existing or future patent rights, nor do the descriptions contained in this document imply the granting of licenses to make, use, or sell equipment or software in accordance with the description. No responsibility is assumed for the use or reliability of firmware on equipment not supplied by Compaq or its affiliated companies. Possession, use, or copying of the software or firmware described in this documentation is authorized only pursuant to a valid written license from Compaq, an authorized sublicensor, or the identified licensor.

Commercial Computer Software, Computer Software Documentation and Technical Data for Commercial Items are licensed to the U.S. Government with Compaq's standard commercial license and, when applicable, the rights in DFAR 252.227 7015, "Technical Data-Commercial Items."

Compaq, the Compaq logo, DIGITAL, DIGITAL UNIX, DECconnect, HSZ, HSG, StorageWorks, VMS, OpenVMS Registered in the United States Patent and Trademark Office.

UNIX is a registered trademark in the United States and other countries exclusively through X/Open Company Ltd. Windows NT is a registered trademark of the Microsoft Corporation. Sun is a registered trademark of Sun Microsystems, Inc. Hewlett-Packard, TACHYON, and HP-UX are registered trademarks of the Hewlett-Packard Company. IBM and AIX are registered trademarks of International Business Machines Corporation. All other trademarks and registered trademarks are the property of their respective owners.

Contents

About This Guide

Chapter 1
Introduction to Disaster Tolerant Solutions

Chapter 2
Getting Started

Chapter 3
Configuring a Data Replication Manager Solution

Chapter 4
Managing and Operating a Data Replication Manager Solution

Chapter 5
Troubleshooting

Figures

Tables

About This Guide

This book describes the functionality of Data Replication Manager running on the HSG80 Array Controller.

See the documentation that accompanied the subsystem for detailed information about subsystem enclosures and their components.

Getting Help

If you have a problem and cannot find the information you need to resolve it in this guide, you can get further information and other help in the following locations:

Compaq Website

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

Telephone Numbers

For Compaq technical support:

In the United States and Canada, call 1-800-652-6672.

For Compaq technical support phone numbers outside the United States and Canada, visit the Compaq Website at: http://www.compaq.com.

Precautions

Follow these precautions when carrying out the procedures in this book:

Electrostatic Discharge Precautions

Static electricity collects on all nonconducting material, such as paper, cloth, and plastic. An electrostatic discharge (ESD) can easily damage a controller or other subsystem component even though you may not see or feel the discharge. Follow these precautions whenever you’re servicing a subsystem or one of its components:

- Always use an ESD wrist strap when servicing the controller or other components in the subsystem. Make sure that the strap contacts bare skin, fits snugly, and that its grounding lead is attached to a bus that is a verified earth ground.
- Before touching any circuit board or component, always touch a verifiable earth ground to discharge any static electricity that may be present in your clothing.
- Always keep circuit boards and components away from nonconducting material.
- Always keep clothing away from circuit boards and components.
- Always use antistatic bags and grounding mats for storing circuit boards or components during replacement procedures.
- Always keep the ESD cover over the program card when the card is in the controller. If you remove the card, put it in its original carrying case. Never touch the contacts or twist or bend the card while you’re handling it.
- Never touch the connector pins of a cable when it is attached to a component or host.

Component Precaution

System components referenced in this manual comply to regulatory standards documented herein. Use of other components in their place may violate country standards, negate regulatory compliance, or invalidate the warranty on your product.

FCC Precautions

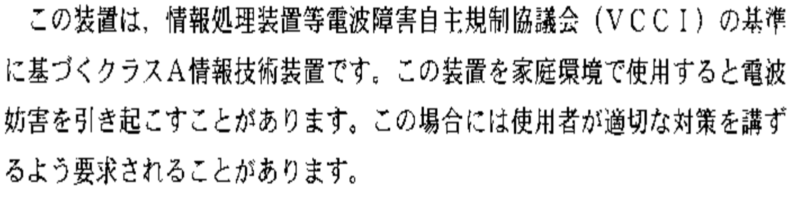
This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the manuals, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense. Restrictions apply to the use of the local-connection port on this series of controllers; failure to observe these restrictions may result in harmful interference. Always disconnect this port as soon as possible after completing the setup operation. Any changes or modifications made to this equipment may void the user’s authority to operate the equipment.

Warning!
This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Achtung!
Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten, in welchen Fällen der Benutzer für entsprechende Gegenmaßnahmen verantwortlich ist.

Attention!
Ceci est un produit de Classe A. Dans un environnement domestique, ce produit risque de créer des interférences radioélectriques, il appartiendra alors à l'utilisateur de prendre les mesures spécifiques appropriées.

JAPAN



この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

USA

This equipment generates, uses, and may emit radio frequency energy. The equipment has been type tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules, which are designed to provide reasonable protection against such radio frequency interference. Operation of this equipment in a residential area may cause interference in which case the user at his own expense will be required to take whatever measures may be required to correct the interference. Any modifications to this device - unless expressly approved by the manufacturer - can void the user's authority to operate this equipment under part 15 of the FCC rules.

Conventions

This book uses the following typographical conventions and special notices to help you find what you're looking for. See page xviii for more details.

Typographical Conventions

Convention	Meaning
ALLCAPS	Command syntax that must be entered exactly as shown and for commands discussed within text, for example: SET FAILOVER COPY=OTHER_CONTROLLER "Use the SHOW SPARESET command to show the contents of the spareset."
Monospaced	Screen display.
Sans serif italic	Command variable or numeric value that you supply, for example: SHOW *RAIDset-name* or SET THIS_CONTROLLER ID=*(n,n,n,n,)*
italic	Reference to other books or publications, for example: "See the *HSG80 Array Controller ACS V8.3 Release Notes* for details."
. . .	Indicates that a portion of an example or figure has been omitted.
"this controller"	The controller serving your current CLI session through a local or remote terminal.
"other controller"	The controller in a dual-redundant pair that's connected to the controller serving your current CLI session.

Special Notices

This book does not contain detailed descriptions of standard safety procedures. However, it does contain warnings for procedures that could cause personal injury and cautions for procedures that could damage the controller or its related components. Look for these symbols when you're carrying out the procedures in this book:

⚠ **WARNING:** A warning indicates the presence of a hazard that can cause personal injury if you do not observe the precautions in the text.

△ **CAUTION:** A caution indicates the presence of a hazard that might damage hardware, corrupt software, or cause a loss of data.

IMPORTANT: A tip provides alternative methods or procedures that may not be immediately obvious. A tip may also alert customers that the controller's behavior being discussed is different from prior software or hardware versions.

NOTE: A note provides additional information that's related to the completion of an instruction or procedure.

Related Publications

The following table lists some of the documents that you will need to refer to when connecting, configuring, and operating your DT solution.

Document Title	Part Number
HSG80 Array Controller ACS V8.4 Configuration and CLI Reference Guide	118619-001 / EK-HSG84-RG
HSG80 Array Controller ACS V8.3/8.4 Maintenance and Service Guide	118629-001 / EK-HSG84-SV
StorageWorks Fibre Channel Storage Switch Service Guide	135268-001 / AA-RHBZA-TE
StorageWorks Fibre Channel Storage Switch User’s Guide	135267-001 / AA-RHBYA-TE
Compaq StorageWorks RA8000 and ESA12000 Storage Subsystems User’s Guide	387404-001 / EK–SMCPR–UG
Compaq Storageworks RA8000 and ESA12000 Fibre Channel Cluster Solutions for Windows NT Installation Guide	101471-001 / EK-NTC8K-IG
RA8000 and ESA12000 HSG80 Solution Software V8.3/V8.4 for WindowsNT Server - Intel Installation Reference Guide	387387-002 / AA-RFA9B-TE
RA8000 and ESA12000 Fibre Channel Storage Subsystem for WindowsNT Server - Intel Quick Setup Guide (for ACS V8.3)	387387-002 / AA-RFA7A-TE
RA 8000 and ESA12000 Fibre Channel Storage Subsystem for WindowsNT Server - Intel Quick Setup Guide (for ACS V8.4)	136258-001 / AA-RHH5A-TE
StorageWorks Secure Path for Windows NT, A High Availability MultiPath Solution Installation Guide	123995-001 / EK-WNTMP-MH
KGPSA PCI-to-Fibre Channel Host Adapter	EK–KGPSA–UG
Compaq StorageWorks Ultra SCSI RAID Enclosure (DS-BA370-Series) User’s Guide	387403–001 / EK–BA370–UG
Command Console Version 2.1 (HSG80) for RA8000/ESA12000 User’s Guide	387405-003 / AA-RFA2C-TE

Data Replication Manager Solutions Kit for Windows NT/Intel

The following components should be included in your Data Replication Manager Solutions Kit (part number QB-6BUAA-SA):

- Compaq StorageWorks Data Replication Manager HSG80 Array Controller ACS Version 8.4P Operations Guide
- Compaq StorageWorks HSG80 Array Controller ACS Version 8.4 Configuration and CLI Reference Guide
- Compaq StorageWorks HSG80 Array Controller ACS Version 8.4 Maintenance and Service Guide
- Command Console V2.1 (HSG80) for RAID Array 8000/ESA 12000 User's Guide
- RA8000/ESA12000 HSG80 Solution Software V8.4 for WindowsNT® - Intel Installation Reference Guide
- RAID Array 8000/ESA12000 Fibre Channel Storage Subsystem for Windows NT® Server - Intel Quick Setup Guide
- RAID Array 8000/ESA12000 Fibre Channel Cluster Solutions for WindowsNT® Installation Guide
- Digital™ StorageWorks Warranty Terms and Conditions
- Compaq StorageWorks Customer Letter
- Compaq License Agreement
- HSG80 Product Registration Card

Revision History

This is a new document.

Chapter 1
Introduction to Disaster Tolerant Solutions

This chapter defines Disaster Tolerant (DT) storage and describes the concept of remote replication.

Introduction to Disaster Tolerance

DT solutions are designed to provide rapid data access recovery and continued data processing after the loss of one or more components. During normal data processing, data is simultaneously written to local and remote sites. The local site is known as the initiator site, or initiator, because it is in control of operations. The remote site is known as the target site, or target. While copies of data reside at both sites, host data access occurs through the initiator site, unless there is a failure or catastrophe that disables processing there. With DT, your operating system can detect hardware and software failures that affect the initiator storage, and in the event of an initiator failure, another site can continue processing data in the interim.

Introduction to StorageWorks Data Replication Manager

Data Replication Manager provides controller-based mirroring across a Fibre Channel link. The HSG80 Array Controller Subsystem is used on a host port-to host port basis, which allows data to be synchronously migrated from one storage subsystem to another, even if they are located at different physical sites.

Synchronous operation provides real-time mirroring of data. In this mode, data is simultaneously written to the cache of the initiator subsystem and the cache of the target subsystems, and the I/O completion status is not sent to the host until all members of the mirrorset are updated. If a member of a remote copy set cannot complete the I/O, then the I/O must fail or the failed member must be removed before the completion status can be returned to the host. With Data Replication Manager, if a mirrorset with two members loses one member, it is not considered DT-safe. The failed member is then removed, and the controller will return vendor-unique Additional Sense Codes and Additional Sense Code Qualifiers (ASC-ASCQ) to the host. Synchronous operation ensures the highest possible level of data consistency, which makes this process especially appropriate for business applications that require a high level of accuracy.

Using the required multiple-bus failover configuration (refer to the *HSG80 Array Controller ACS Version 8.4 Configuration and CLI Reference Guide* for more detail), the controller is not only able to distribute an I/O request to both the initiator and target sites, but it can also transfer the initiator's role to the target as needed. Thus, Data Replication Manager is a distributed computing model that supports full Disaster Tolerant storage.

Required Hardware and Software

Table is a checklist of equipment that is mandatory for operating a DT storage subsystem with Data Replication Manager

Use this list to verify that you have everything, or you may not be able to configure your system to replicate data in a DT subsystem.

Table 1–1 Hardware and Software Requirements Checklist and Part Numbers

Required Hardware	**Part Number**	**Quantity** (at each site)	✔
ESA12000	380590–B21 (50 HZ, blue) 380590–B22 (50 HZ, opal) 380580–001 (60 HZ, blue) 380580–002 (60 HZ, opal)	Minimum of 1	
Fibre channel gigabit switch			
8-port	380591–B21 / DS–DSGGA–AA	2	
16-port	380578–B21 / DS–DSGGA–AB		
Host bus adapter	380574–001/ KGPSA–BC	2 (per system)	

Table 1–1 Hardware and Software Requirements Checklist and Part Numbers (Continued)

Fibre Channel host cables 5 meters 15 meters 30 meters 50 meters	234457–B22 / BNGBX–05 234457–B23 / BNGBX–15 234457–B24 / BNGBX–30 234457–B25 / BNGBX–50	2	
Fibre Channel controller cables (2 meters)	234457–B21 / DS–BNGBX–02	4	
Short-wave Gigabit Interface Converters (GBICs)	380561–B21 / DS–DXGGA–SA	6	
Long-wave Gigabit Interface Converters (GBICs)	127508–B21 / DS–DSGGA–MA	2	
SIte-to-Site Single Mode Cable	N/A	2	

Required Software	Part Number	✔
ACS V8.4P	128698–B21 / QB–6CAAA–SA	
Secure Path 2.1	380594–001 / QB–6695A–AA	
SWCC Version 2.1 (optional)	N/A	

Subsystem Components

The Data Replication Manager storage subsystem consists of an initiator site and a target site that are linked together with up to 10 kilometers of fiber optic cable. The Fiber Channel gigabit switches connect the array controller ports at each site. In the event of a disaster at the initiator site, data processing is moved from the initiator site to a target site through a site failover. When problems at the initiator site have been resolved, data processing can be transferred back to the original initiator site through a site failback. See Chapter 5 for a full explanation on failover and failback. Because the hardware and software used to implement Data Replication Manager is segmented between the initiator and target sites, it is imperative that the host processor at the target site be capable of running the same application as the initiator site host.

Hardware Components

The DT configuration that supports Data Replication Manager involves two HSG80 array controller subsystems-one at the initiator site and one at the target site. Each site houses one or more ESA12000 cabinet that is equipped with one or more BA370 enclosure and disk Storage Building Blocks (SBBs). Each BA370 enclosure holds 24 disks.

NOTE: Data Replication Manager can run with cabinets that have 24, 48, or 72 (requires two cabinets) disk drives, but the initiator and target sites must be equipped with the identical number of disks.

The hosts at the initiator and target sites are connected to a pair of dual redundant HSG80 array controllers, which are located inside of these enclosures. See the *RA8000 and ESA12000 Storage Subsystems User’s Guide* for complete details on this equipment.

NOTE: While this documentation addresses ESA12000 storage cabinets as the primary unit for Data Replication Manager configurations, Compaq’s DT solution will function in any equivalent cabinet that houses a BA370 enclosure.

Connections between the controllers and hosts are made at each site with two Fibre Channel gigabit switches and two host bus adapters. Short-wave Gigabit Interface Converters (GBICs) connect the host and controllers to the switches at each site. Long-wave GBICs connect the initiator and target switches together if they are more than 500 meters apart. See Chapter 2 for information on how to install and operate these components.

ESA12000 Cabinet

The ESA12000 Storage Building Block Cabinet houses the BA370 Enclosures, which contain the following components:

- Two HSG80 Fibre Channel RAID Array Controllers
- One Environmental Monitoring Unit (EMU)
- One or Two AC Input Power controllers
- Up to 24 Disk Drive Storage Building Blocks (SBB) per BA370 Enclosure
- Five to Eight 180-watt Power Supplies
- External Cache Battery (ECB), dual
- Eight Cooling Fans
- Six single-ended I/O Modules
- One Power Verification and Addressing module (PVA)
- Two cache modules (512 MB required)

For detailed information about these components, refer to the *HSG80 Array Controller ACS Version 8.4 Configuration and CLI Reference Guide* and the *HSG80 Array Controller ACS Version 8.4 Maintenance and Service Guide*.

Figure 1–1 shows these parts inside the ESA12000 cabinet with a 24 disk drive capacity. Subsequent sections outline additional hardware requirements needed to complete the Data Replication Manager solution.

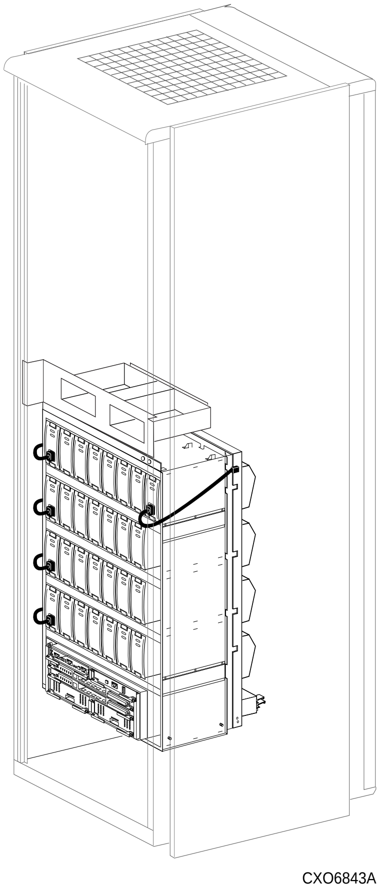


Figure 1–1. ESA12000 Storage Building Block

Figure 1–2 highlights the specific components that must be added to the ESA 12000 building block to support a Data Replication Manager solution.

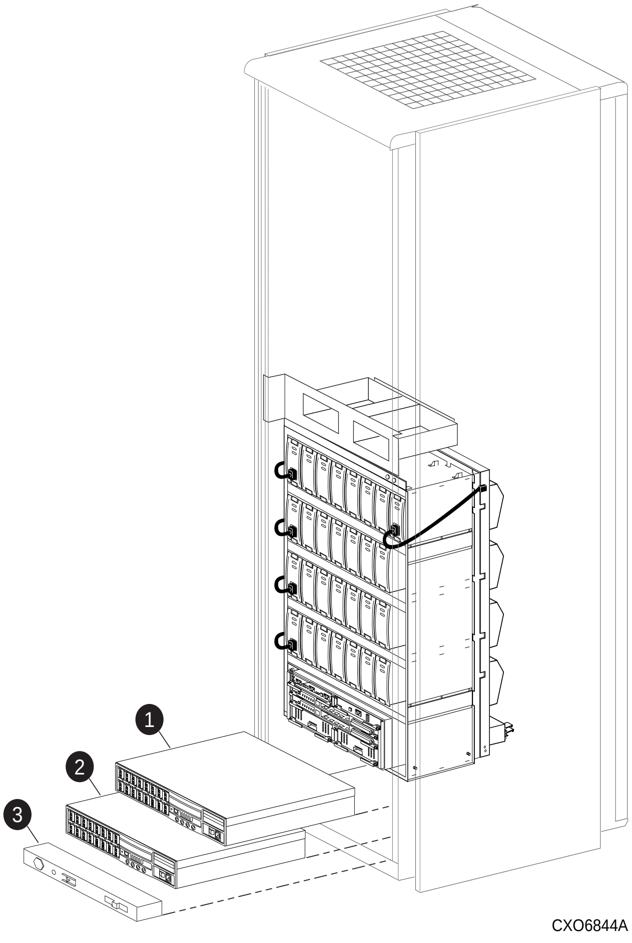


Figure 1–2. Additional Components for Data Replication Manager

Table 1–2 Key to Figure 1–2 Additional Components Required for Data Replication Manager

Item	Description
❶	Top Fibre Channel Gigabit Switch, 8- or 16-port
❷	Bottom Fibre Channel Gigabit Switch, 8- or 16- port
❸	Redundant Power Distribution Unit (optional)

The following sections outline the components that are specific to the disaster tolerant solution.

Fibre Channel Gigabit Switch

The Fibre Channel gigabit switch, shown in Figure 1–3 is used to connect the controllers to the hosts and to link the initiator and target sites together. The ports hold short- or long-wave Gigabit Interface Converters, which are described in the next section. See the *StorageWorks Fibre Channel Storage Switch User’s Guide* for an in-depth look at the features and functions of the Fibre Channel gigabit switch.

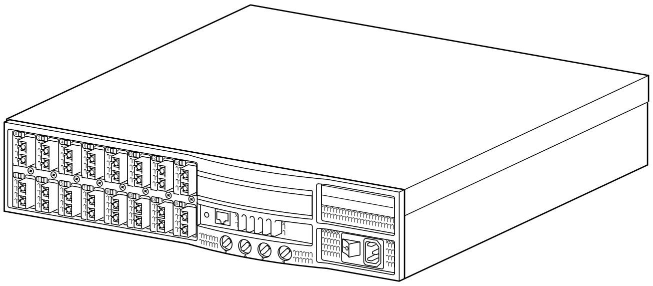


Figure 1–3. Fibre Channel Gigabit Switch

Gigabit Interface Converters (GBIC)

GBICs are the converters that are inserted into the ports of the Fibre Channel switch and serve as the interface between the fiber optic cables and the switch. Short-wave GBICs are used with a 50 micron multi-mode fiber optic cable (SC-terminated) to connect the components at the initiator and target sites (host-to-switch; controller-to-switch). The maximum distance that short-wave GBICs support is 500 meters. Long-wave GBICs are used with 9 micron single-mode fiber optic cables (SC-terminated) to link the initiator and target sites together. Long-wave GBICs connect switches that are up to 10 kilometers apart. See the *StorageWorks Fibre Channel Storage Switch User's Guide* to learn more about GBICs.

Power Distribution Unit (PDU)

The PDU is another component that is included with the ESA12000 cabinet and is used to distribute power to the BA370s and switches. A second PDU can be ordered to support a fully-redundant power configuration. See the *RA8000 and ESA12000 Storage Subsystems User's Guide* for more detailed information.

Fully-Redundant Power—Optional

Fully-redundant power is an optional feature designed to offer a more secure source of power in the event that one or more units should fail. If less than five power components are operational, then the entire cabinet will shut down. This requires three additional power supplies and one additional AC power controller that plugs into one additional PDU. These additional components must be supplied for each BA370 enclosure. See the *RA8000 and ESA12000 Storage Subsystems User's Guide* for more details about power supply Storage Building Blocks (SSBs).

Host Bus Adapter

The host bus adapters are inserted into the available slots on the host computer's PCI Bus. A Fibre Channel connection is made by inserting a multi-mode fiber optic cable between each adapter and an individual port on the Fibre Channel switch. See the *KGPSA PCI-to-Fibre Channel Host Adapter* guide for more information.

Final Assembly

Your final DT setup should reflect Figure 1–4.

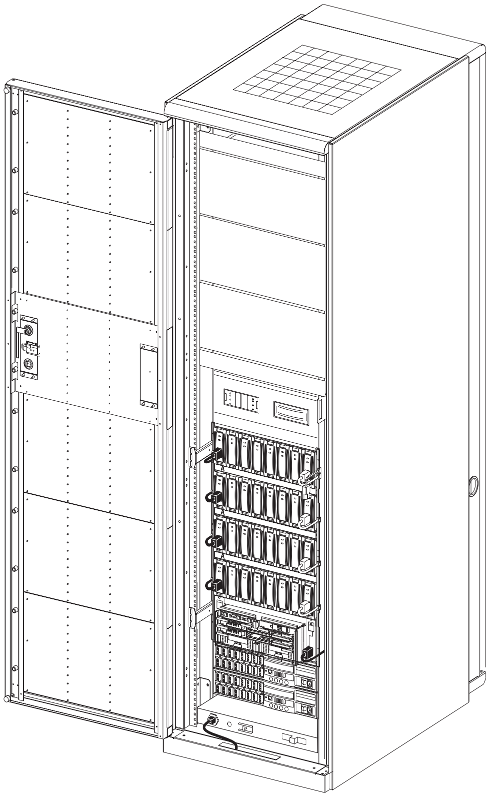


Figure 1–4. Fibre Channel-Based DT Storage Subsystem (with Fully-Redundant Power)

NOTE: If you prefer to join cabinets for more storage capacity, follow the instructions in the *RA8000 and ESA12000 Storage Subsystems User's Guide*, and be sure to establish the same setup at both the initiator and target sites. Keep in mind that an additional cabinet will not include switches or controllers. It will, however, hold a PDU and be able to support redundant power.

Software Components

This section describes the software components necessary to configure and manage a DT storage subsystem. For installation instructions, see Chapter 2. The following list shows the software required to enable Data Replication Manager:

- Array Controller Software (ACS) Version 8.4P
- Secure Path Version 2.1 (Required for Windows NT)
- Storage Works Command Console (SWCC) Version 2.1 (optional)

Array Controller Software

The HSG80 Array Controller Software (ACS) is the software component of the HSG80 array controller subsystem. ACS software executes on the HSG80 controller and processes I/O requests from the host, performing the device level operations required to satisfy the requests.

Secure Path

Secure Path is server-based software that enhances the StorageWorks RAID dual-ported storage subsystem by providing automatic error recovery from server-to-storage subsystem connection failures. Secure Path allows you to add redundant Fibre Channel paths between Windows NT hosts and a RAID storage subsystem, improving overall data availability. If any component in the path between the host and storage subsystem fails, Secure Path immediately redirects all pending and subsequent I/O requests from the failed path to an alternate path, preventing an adapter, cable, or controller failure from disrupting data access.

For more information on Secure Path, refer to the *SecurePath for Windows NT® Installation Guide*.

StorageWorks Command Console

SWCC provides local and remote management of StorageWorks controllers and their attached storage. SWCC consists of two major components: the SWCC client and the SWCC agent. SWCC can be used to configure and manage the DT storage subsystem.

The SWCC client is a graphical user interface (GUI) that runs on a local host and displays the logical and physical layout and status of a selected subsystem in graphical form.

The agent is a companion program to the client. This host-resident program is an interface between the client and the host’s storage subsystem that allows the two to communicate over a network.

For a full description of SWCC and how it operates, refer to the *StorageWorks Command Console Getting Started Guide*.

Chapter 2
Getting Started

This chapter explains how to set up your DT subsystem and run the Data Replication Manager solution.

NOTE: It a good idea to keep a copy of this manual at both the initiator and target sites, so as to ensure a successful and identical setup at both sites. Two copies will also eliminate confusion if more than one person is configuring Data Replication Manager.

Site, Host, and Solution Preparation

Before you start operating your DT subsystem, you will need to ensure that you have enough clearance to install and store the subsystem(s) and have adequate power resources. If you choose to use more than one cabinet, you will need to understand the proper methods for positioning and joining them. In addition, you will need to have the proper devices installed and verify that all of the BA370 components are in place.

To learn more about adding additional storage, refer to the *RA8000 and ESA12000 Storage Subsystems User's Guide*.

Host Bus Adapter Requirements

To run your Data Replication Manager solution, you must have two host bus adapters installed into your host system. Refer to the *KGPSA PCI-to-Fibre Channel Host Adapter* guide that came with your adapter for detailed information on this hardware.

At this time, it is important to locate and record the worldwide names of each host bus adapter. For the host bus adapter at the target site, you can record the worldwide name in the worksheet provided on 3–22. The initiator site host bus adapter worldwide names can be recorded in the worksheet found on page 3–42. You will need to have this number handy when you rename the host connections in Chapter 3.

NOTE: The worldwide name can be found on the bottom of the host bus adapter board. Look for a small bar code label with an IEEE (Institute of Electrical and Electronics Engineers) precursor.

Setting Up the Fibre Channel Switches

The Fibre Channel gigabit switch must be in place before the subsystems can be cabled and configured. You will need the following to install your Fibre Channel switches:

- Power cord

- 10BASE-T cable with RJ45 plug (to be connected to a low-cost Ethernet hub or switch)
- Fixed IP address and subnetmask (one of each per switch)

The Ethernet cable and IP address are required to monitor and administer the Fibre Channel switch. You will have to configure the Ethernet IP address and the Ethernet IP subnet mask with the front panel buttons of the Fibre Channel switch. See the *StorageWorks Fibre Channel Storage Switch User's Guide* for more details.

Once the Ethernet IP settings are established, verify that the Ethernet is operating by performing the following steps:

1. Update the *\winnt\system32\drivers\etc\hosts* file with the IP address and the name of the Fibre Channel switch.
2. *Ping* using the Ethernet IP address of the switch. If this is successful, you have access to the switch.
3. *Ping* using the name of the switch. This will verify the operation of the name resolution.
4. *Telnet* into the switch with the password *admin*, and make the following adjustments to the switch:
   - ❑ Type *switchName* to configure the switch name. Be sure to designate a name that will enable you to easily identify the switch that you are trying to access.
   - ❑ Type *switchShow* to reveal the status of the switch and some of its ports.
   - ❑ Type *version* to display the firmware levels. You must be running version 1.6B or higher.
5. Using, a Java-capable browser, go to *http://<FC switch DNS name>* to view a visual representation of the switch. You can double-click on this picture for further information.

Setting Up the Fiber Optic Cables

Before you connect the fiber optic cables to your subsystems, it is important to understand the designated names of each component. Figure 2–1 shows what each component will be referred to in this document:

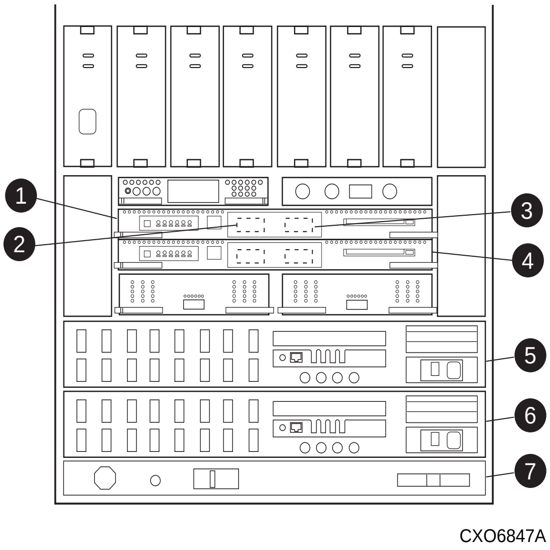


Figure 2–1. Component Locations and Names

Table 2–1 Key to Figure 2–1 Component Locations and Names

Item	Description
❶	Controller A
❷	Port 1 on Controller A
❸	Port 2 on Controller A
❹	Controller B
❺	Top Fibre Channel Switch
❻	Bottom Fibre Channel Switch
❼	Redundant PDU

Before you connect the fiber optic cables, Compaq recommends that you tag each end of the cables with the following information:

Host-to-Switch Connection

- Rank number or PCI slot number of the host bus adapter
- Port number on switch

Switch-to-Controller Connection

- Fibre Channel switch name (top or bottom)
- Fibre Channel switch port number (0-15)
- Site name (initiator or target)
- Controller name (A or B)
- Controller port number (1 or 2)
- Host port number
- Host Bus Adapter worldwide name

The DT solution requires two different types of fiber optic cables, depending on where the connections are made. Cabling at each individual site that involves the controller, the switch, and the host is made with 50 micron multi-mode fiber optic cables. The maximum length that these cables will support is 500 meters. When cabling between initiator and target sites that are more than 500 meters apart, you must use a 9 micron single-mode fiber optic cable, which can run a distance of up to 10 kilometers.

CAUTION: If the Fibre Channel optical cable is not properly connected to the controller, failure may result. Because of the cable's frail nature, it must also be regularly maintained, or its performance and life span will be affected. Before proceeding, it is important to administer the precautionary measures detailed in the *HSG80 Array Controller ACS Version 8.4 Maintenance and Service Guide.*

The sequence of connections can be made in any order, but here is an overall look at the connections that you will need to make at and between each site:

Initiator Site			**Target Site**		
Host Port	→	Top Switch, Port 0	Host Port	→	Top Switch, Port 0
Host Port	→	Bottom Switch, Port 0	Host Port	→	Bottom Switch, Port 0
Controller A, Port 1	→	Top Switch, Port 2	Controller A, Port 1	→	Top Switch, Port 2
Controller A, Port 2	→	Top Switch, Port 4	Controller A, Port 2	→	Top Switch, Port 4
Controller B, Port 1	→	Bottom Switch, Port 2	Controller B, Port 1	→	Bottom Switch, Port 2
Controller B, Port 2	→	Bottom Switch, Port 4	Controller B, Port 2	→	Bottom Switch, Port 4

Between Initiator and Target Sites				
Top Switch, Port 6	→	External Fiber Link	←	Top Switch, Port 6
Bottom Switch, Port 6	→	External Fiber Link	←	Top switch, Port 6

Chapter 3
Configuring a Data Replication Manager Solution

Chapter 3 explores various configuration options and outlines standard operating procedures for your Data Replication Manager solution.

Introduction

The DT configuration that supports Data Replication Manager involves two HSG80 array controller subsystems—one at an initiator site and one at a target site.

IMPORTANT: Because of the complexity of the configuration process, it is a good idea to have all Data Replication Manager documentation available at both sites to eliminate confusion and minimize the risk of error.

Restrictions

It is important to understand the operating restrictions before configuring your Data Replication Manager solution. Table 3–1 lists the points to consider when proceeding to the configuration process:

Table 3–1 Restrictions

Restriction	Implication
Two HSG80 controller pairs are required	All controllers must run ACS V8.4P
Four Fibre Channel Switches are required	These switches provide the connection between controllers at the initiator and target sites
HSG80 controller(s) must be configured in Multiple-Bus Failover mode	Additional software support required on the host. ■ Windows NT: Secure Path V2.1 or higher ■ Open VMS: OpenVMS V7.2/Alpha
HSG80 controller(s) must be configured for Fibre Channel Switched protocol	Host operating system and adapter must support Fibre Channel Switched protocol as well
Mirrored write-back Cache must be enabled	■ 512 M cache per controller ■ 256 M mirrored cache
Maximum of 8 Remote Copy Sets allowed per HSG80 controller	If more than 8 Remote Copy sets are needed, additional controller pairs are required
Maximum of 2 members allowed per Remote Copy Set (1 initiator; 1 target)	Composed of 1 initiator and one target
Minimum Chunksize is 64	for RAID 5, RAID0+1, and RAID 0

Table 3–1 Restrictions (Continued)

Restriction	Implication
Only one initiator and one target allowed	2 sites
Target cannot reside on the same controller pair as its initiator	One controller pair required for initiator; one controller pair required for target
Controller replication conducted through port 2 on each controller	■ Link between initiator and target site is made through Port 2 ■ Both link must be up when configured
Each controller pair creates 4 connection IDs on its partners	Number of connections reduced from 32 to 28 if the target site has a controller pair
It is not possible to run DILX on units used by Remote Copy Sets	Run DILX prior to creating the Remote Copy Set configuration
The LUN/unit at the initiator and target sites must be exactly the same size.	Keep the unit number, RAID level, disks used, etc. the same to eliminate confusion and error risk.
Must perform a SAVE_CONFIGURATION after the target and initiator sites have been configured.	Failback cannot occur unless a SAVE_CONFIGURATION has been implemented. See the *HSG80 Array Controller ACS Version 8.4 Configuration and CLI Reference Guide* for details.
Controller-based partitions are not supported within Remote Copy Sets	Host software may be capable of partitioning units.
Unit at the initiator and target sites cannot be transportable units	Units cannot be moved to non-controller configurations without potential data loss.
Cannot use FRUTIL on remote site while I/O is in progress to target site	

Configuring

Both the initiator and the target sites need some type of CLI interface to the controller. You can either connect the serial maintenance port of both the initiator and target site controllers to a terminal from which you issue CLI commands, or you can connect each controller's serial maintenance port to the COMM port of the Windows NT system at both sites. The latter would require the use of terminal emulation software to simulate the function of a terminal.

The procedures for configuring a DT system using the controller's serial maintenance port and CLI commands are as follows:

- Configure the Controllers at the Target Site
- Configure the Storage at the Target Site
  - ❑ Devices and StorageSets
  - ❑ LUNs
  - ❑ Connect Fiber Optic Cables Between the Controllers and Switches
  - ❑ Connect the Target Site to the External Fiber Link
  - ❑ Configure the Host
    - ❑ Install the Host Bus Adapters and Drivers
    - ❑ Install Windows NT (optional)
    - ❑ Install Secure Path
    - ❑ Install SWCC (optional)
    - ❑ Connect Fiber Optic Cables Between the Hosts and the Switches
    - ❑ Rename the Host Connections
- Configure the Controllers at the Initiator Site
- Configure the Storage at the Initiator Site
  - ❑ Devices and StorageSets
  - ❑ LUNs
  - ❑ Connect Fiber Optic Cables Between the Controllers and Switches
  - ❑ Connect the Initiator Site to the External Fiber Link
  - ❑ Create Remote Copy Sets
  - ❑ Set Failsafe at the Initiator Site (optional)
  - ❑ Save Configuration to a Disk
  - ❑ Configure the Host
    - ❑ Install the Host Bus Adapters and Drivers

- ❏ Install Windows NT (optional)
- ❏ Install Secure Path
- ❏ Install SWCC (optional)
- ❏ Connect Fiber Optic Cables Between the Hosts and the Switches
- ❏ Rename the Host Connections
- ❏ Enable Access to the Hosts

- ■ Verify System Operation
  - ❏ Install Cluster Server for Windows NT (optional)

Each of these steps are detailed in the following sections.

Configure the Controllers at the Target Site

Prior to configuring the controllers at the target site, be sure to follow these preparatory steps:

- Identify the world wide name on the host bus adapters. See page 2–2 for instructions on how to locate this name.
- Establish the name that you will assign to the target site.

The first step to getting your DT system up and running involves setting up and configuring the controllers. These tasks are outlined below:

1. Ensure that all BA370 enclosures, Fibre Channel switches, power distribution units (PDUs), and the main power supply are off.
2. Plug all cabinet PDU power cords into the main power receptacles.
3. Be sure that you have a serial connection to each of the controllers.
4. Apply power to the main power source.
5. Turn on all PDUs.
6. Ensure that the switches are powered on but not cabled.
7. Turn on the BA370 cabinets.

   NOTE: When the BA370 cabinets are turned on, the controllers will boot if the PCMCIA cards are already installed. If there are no cards in the controller slots, insert them now, and depress the reset button. Refer to the *HSG80 Array Controller ACS Version 8.4 Configuration and CLI Reference Guide* for complete instructions on how to properly seat the controller cards.
8. Establish a local connection to the controller. Refer to the *HSG80 Array Controller ACS Version 8.4 Maintenance and Service Guide* for instructions.
9. Verify that all controllers are on and functional by looking for the CLI prompt on the maintenance port terminal.

   NOTE: Unless otherwise noted, all operations may be conducted from controller A.
10. Issue the following CLI command:

```
SHOW THIS
```

You will see a display similar to the following:

```
Controller:
       HSG80 ZG8nnnnnnn Software R0nnP-0, Hardware  E03
       NODE_ID          = nnnn-nnnn-nnnn-nnnn
       ALLOCATION_CLASS = 0
       SCSI_VERSION     = SCSI-2
       Not configured for dual-redundancy
         Controller misconfigured -- other controller present
       Device Port SCSI address 7
       Time: NOT SET
       Command Console LUN is disabled
Host PORT_1:
       Reported PORT_ID = nnnn-nnnn-nnnn-nnnn
       PORT_1_PROFILE   = PLDA
       PORT_1_TOPOLOGY  = OFFLINE (offline)
Host PORT_2:
       Reported PORT_ID = nnnn-nnnn-nnnn-nnnn
       PORT_2_PROFILE   = PLDA
       PORT_2_TOPOLOGY  = OFFLINE (offline)
       NOREMOTE_COPY
Cache:
       512 megabyte write cache, version 0012
       Cache is GOOD
       No unflushed data in cache
       CACHE_FLUSH_TIMER = DEFAULT (10 seconds)
Mirrored Cache:
       Not enabled
Battery:
       FULLY CHARGED
       Expires:           WARNING! UNKOWN EXPIRATION DATE!
       WARNING: AN UNKNOWN NUMBER OF DEEP DISCHARGES HAVE OCCURRED!
       NOCACHE_UPS
Controllers misconfigured. Type SHOW THIS_CONTROLLER
```

11. Verify that the subsystem worldwide name is set. If it is, go to step 15. If the worldwide name has not been assigned to the controller, you will need to obtain the name and set it before proceeding.

    NOTE: The subsystem’s worldwide name can be found on a sticker, which is located on top of the frame that houses the controllers, the EMU, the PVA, and the cache modules. If there is no label there, contact your Compaq customer service representative for assistance. Refer to the *HSG80 Array Controller ACS Version 8.4 Configuration and CLI Reference Guide* for more information on worldwide names.

CAUTION: If you attempt to set the subsystem worldwide name to a name other than the one that came with the subsystem, the data on the subsystem will not be accessible. Never set two subsystems to the same worldwide name, or data corruption will occur.

12. Once the worldwide name has been located, assign it to the controller using the following CLI command:

    ```
    SET THIS NODE_ID=node ID
    ```

    The display should reflect the following:

```
Warning 4000: A restart of this controller is required before all the
       parameters modified will take effect
%CER--HSG80> --09-FEB-1999 10:07:54-- Restart of this controller required
Restart of this controller required
```

13. Restart the controller using the following CLI command:

    ```
    RESTART THIS
    ```

NOTE: Once you have restarted the controller, you will see a series of %LFL, %CER, and %EVL prompts. These indicate a Last Failure Log, a CLI Event Report, and an Event Log, respectively. For a complete explanation of these event reports, refer to the *HSG80 Array Controller ACS Version 8.4 Maintenance and Service Guide*.

14. Issue a SHOW THIS command to verify that the worldwide name has been set. You should see a display similar to the following:

```
Controller:
            HSG80 ZG8nnnnnnn Software R0nnP-0, Hardware  E03
            NODE_ID          = nnnn-nnnn-nnnn-nnnn
            ALLOCATION_CLASS = 0
            SCSI_VERSION     = SCSI-2
            Not configured for dual-redundancy
                Controller misconfigured -- other controller present
            Device Port SCSI address 7
            Time: NOT SET
                        Command Console LUN is disabled.
            .
            .
            .
```

15. Check to see what failover mode the controller is in by looking for a configuration message in the display. Use the following CLI command:

    ```
    SHOW THIS
    ```

    a. If the controller is in multiple bus failover mode, go to step 18.

    b. If the controller is in transparent failover mode, issue the following CLI command:

       ```
       SET NOFAILOVER
       ```

       Proceed to step c.

    c. If the controllers are not configured for any failover mode, issue the following CLI command:

       ```
       SET MULTIBUS_FAILOVER COPY=THIS_CONTROLLER
       ```

       This command automatically reboots the “other” controller.

       You will see a %LFL and a %EVL prompt. Refer to the *HSG80 Array Controller ACS Version 8.4 Maintenance and Service Guide* for more details on these reports.

16. To ensure that the settings from step 15 have been applied, enter:

    ```
    SHOW THIS FULL
    ```

    The output will show that the controllers have been configured to support multiple bus failover mode:

    ```
    Controller:
           HSG80 ZG8nnnnnnn Software R0nnP-0, Hardware  E03
           NODE_ID          = nnnn-nnnn-nnnn-nnnn
           ALLOCATION_CLASS = 0
           SCSI_VERSION     = SCSI-2
           Configured for MULTIBUS_FAILOVER with ZG8nnnnnnn
             In dual-redundant configuration
           Device Port SCSI address 7
           Time: NOT SET
           Command Console LUN is disabled
           .
           .
           .
    ```

NOTE: These settings will automatically be applied to controller B. Therefore, it is not necessary to repeat these steps again on controller B.

17. Verify that the settings have been accepted on controller B by using the following CLI command:

    ```
    SHOW OTHER FULL
    ```

18. Change your controller prompts to help you easily identify which controller you are working on. Enter the following CLI commands:

    ```
    SET THIS_CONTROLLER PROMPT=
    SET OTHER_CONTROLLER PROMPT=
    ```

NOTE: Be sure to specify a meaningful *TargetName*. Do not use “local” and “remote”; these are reserved keywords. The name can be up to eight characters and must be unique to all of your controllers. Follow the naming guidelines as specified in the *HSG80 Array Controller ACS Version 8.4 Configuration and CLI Reference Guide*.

19. If you are not working in a Windows NT environment, proceed to step 23. If you are using Windows NT, check to see if the Command Console LUN (CCL) is disabled. Use the following CLI command:

    ```
    SHOW THIS
    ```

20. If CCL is not disabled, issue the following CLI command:

    ```
    SET THIS NOCOMMAND_CONSOLE_LUN
    ```

21. Verify that the CCL has been disabled by using the following CLI command:

    ```
    SHOW THIS
    ```

The display will indicate that the CCL has been disabled:

```
Controller:
    HSG80 ZG8nnnnnnn Software R0nnP-0, Hardware  E03
    NODE_ID          = nnnn-nnnn-nnnn-nnnn
    ALLOCATION_CLASS = 0
    SCSI_VERSION     = SCSI-2
    Configured for MULTIBUS_FAILOVER with ZG8nnnnnnn
        In dual-redundant configuration
    Device Port SCSI address 7
    Time: NOT SET
    Command Console LUN is disabled
.
.
.
```

22. Verify that the settings you have established from controller A have been applied to controller B by using the following CLI command:

    ```
    SHOW OTHER
    ```

23. Check to see if mirrored write-back cache is enabled by using the following CLI command:

    ```
    SHOW THIS
    ```

    If it is not enabled, issue the following CLI command:

    ```
    SET THIS_CONTROLLER MIRRORED_CACHE
    ```

    The controllers will reboot after mirrored write-back cache has been set, and you will see %LFL and %EVL displays.

24. After the controllers reboot, issue the following CLI command to confirm that mirrored write-back cache is enabled:

    ```
    SHOW THIS
    ```

Notice that mirrored write-back cache is now set:

```
.
.
.
Mirrored Cache:
       256 megabyte write cache, version 0012
       Cache is GOOD
       No unflushed data in cache
.
.
.
```

It is not necessary to repeat this step on controller B.

25. Set the fabric topology for each port on both controllers using the following CLI commands:

    NOTE: You will be prompted to restart the controllers after each command, but you do not need to reboot the controllers until all topologies have been set.

    ```
    SET THIS_CONTROLLER PORT_1_TOPOLOGY=FABRIC
    SET THIS_CONTROLLER PORT_2_TOPOLOGY=FABRIC
    SET OTHER_CONTROLLER PORT_1_TOPOLOGY=FABRIC
    SET OTHER_CONTROLLER PORT_2_TOPOLOGY=FABRIC
    ```

26. Restart the controllers (in this order) with the following CLI commands:

    ```
    RESTART OTHER_CONTROLLER
    RESTART THIS_CONTROLLER
    ```

27. To ensure that fabric is up and running, issue the following CLI command:

```
            SHOW THIS
.
.
.
Host PORT_1:
    Reported PORT_ID = nnnn-nnnn-nnnn-nnnn
    PORT_1_PROFILE   = PLDA
    PORT_1_TOPOLOGY  = FABRIC (fabric up)
    Address     =nnnnnn
Host PORT_2:
    Reported PORT_ID = nnnn-nnnn-nnnn-nnnn
    PORT_2_PROFILE   = PLDA
    PORT_2_TOPOLOGY  = FABRIC (fabric up)
    Address     =nnnnnn
    NOREMOTE_COPY
.
.
.
```

28. You are now ready to enable Data Replication Manager. Use the following CLI command:

```
            SET THIS_CONTROLLER REMOTE COPY=TargetName
```

    After you have entered this CLI command, you will see a series of %LFL and %EVL displays, and the controllers will automatically reboot.

29. Use the following CLI command to verify that these settings are in place:

```
            SHOW THIS
.
.
.
Host PORT_2:
    Reported PORT_ID = nnnn-nnnn-nnnn-nnnn
    PORT_2_PROFILE   = PLDA
    PORT_2_TOPOLOGY  = FABRIC (fabric up)
    REMOTE_COPY = INITR
```

Configure the Storage at the Target Site

Devices and StorageSets

Before you can configure the storage for Data Replication Manager, you need to add the disks, create the RAIDsets, and create units. Follow the instructions in the *HSG80 Array Controller ACS Version 8.4 Configuration and CLI Reference Guide*, but note the restrictions listed at the beginning of this chapter.

NOTE: Keep in mind that the target site must have the same exact storageset and unit configuration that the initiator site will have.

LUNs

Before you can configure the storage at the target site, you must first configure the LUNs. Refer to the *HSG80 Array Controller ACS Version 8.4 Configuration and CLI Reference Guide* for detailed information.

Once all of the units and LUNs have been created, you can proceed to the steps below.

1. Disable access on all units with this command:

   SET *Unit* DISABLE_ACCESS_PATH=ALL

   NOTE: Be sure to issue this command for all units.

2. Verify that the access on each unit is set to none by using the following CLI command:

   ```
   SHOW UNIT FULL
   ```

The display will be similar to the following:

```
LUN                                      Uses             Used by
-------------------------------------------------------------------------------

D110                                 DISK1000
  LUN ID:      nnnn-nnnn-nnnn-nnnn-nnnn-nnnn-nnnn-nnnn
  NOIDENTIFIER
  Switches:
    RUN                     NOWRITE_PROTECT        READ_CACHE
    READAHEAD_CACHE         WRITEBACK_CACHE
    MAXIMUM_CACHED_TRANSFER_SIZE = 32
  Access:
    None
  State:
    ONLINE to this controller
    Not reserved
    NOPREFERRED_PATH
  Size: nnnnnnnn blocks
  Geometry (C/H/S): ( 7000 / 20 / 254 )
.
.
.
```

3. Distribute the units by setting their preferred path. Use either of the following CLI commands:

   SET *Unit* PREFERRED_PATH=THIS_CONTROLLER

   SET *Unit* PREFERRED_PATH=OTHER_CONTROLLER

   NOTE: The target controller should have the same preferred path that the initiator will have.

   Keep the busiest LUNs on different host ports, and remember to reboot the controllers after configuring the LUNs. Otherwise, the preferred path settings will not go into effect.

4. The target units will need to allow access to the controllers at the initiator site. Enable access with this CLI command:

SET *UnitNumber* ENABLE_ACCESS_PATH=(*InitiatorControllerConnection*C,*InitiatorControllerConnection*D*)*

   NOTE: *InitiatorC* and *Initiator D* are ports 2 on the controller. Be sure to repeat this command for each *UnitNumber.*

5. Verify that the target units have access to the initiator controller with this CLI command:

   ```
   SHOW REMOTE FULL
   ```

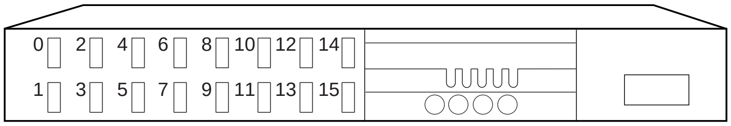
   All remote copy sets should be normalizing.

6. To ensure that your storage settings are in place, use the following CLI command:

   ```
   SHOW STORAGE FULL
   ```

Connect Fiber Optic Cables Between the Controllers and Switches

To better understand which ports you will be instructed to connect the cables to, remember that the port locations on the switch are as follows:



CXO6871A

1. Connect a short-wave, 50 micron fiber optic cable from port 1 of controller A to port 2 of the top Fibre Channel switch.
2. Connect a second short-wave, 50 micron fiber optic cable from port 2 of controller A to port 4 of the top Fibre Channel switch.
3. Connect a third short-wave, 50 micron fiber optic cable from port 1 of controller B to port 2 of the bottom Fibre Channel switch.
4. Connect a fourth short-wave, 50 micron fiber optic cable from port 2 of controller B to port 4 of the bottom Fibre Channel switch.

NOTE: You should see an illuminated LED on the switch as soon as the cable is inserted. This verifies that there is a good connection.

Figure 3–1 illustrates what your cabling should look like. The numbered callouts reflect the steps that you just completed.

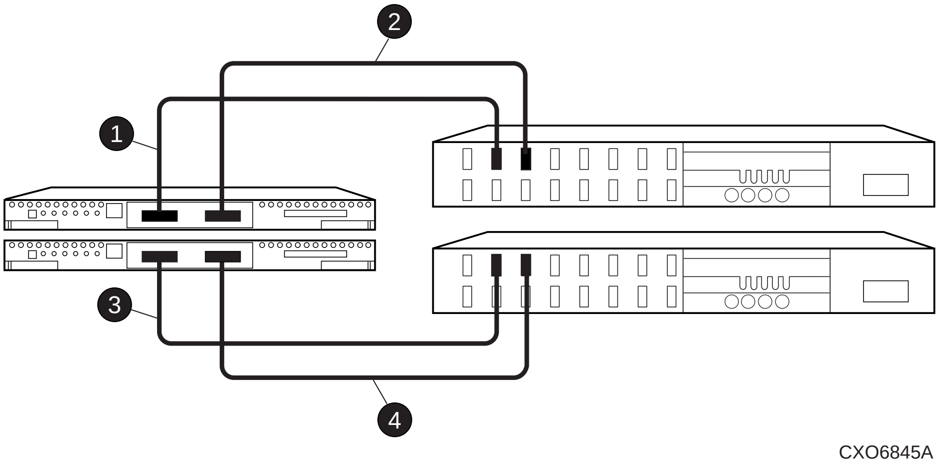


Figure 3–1. Cabling Between the Controllers and Switches

Connect the Target Site to the External Fiber Link

1. Locate the connection points at the target site that link the target site to the initiator site. Look for either a fiber optic cable connector or a patch panel where you can insert a cable.
2. Connect a long-wave, 9 micron fiber optic cable from port 6 of the top switch to one connection point.
3. Connect another long-wave, 9 micron fiber optic cable from port 6 of the bottom switch to the other connection point.

The target site is now physically linked to the initiator site. See Figure 3–2 for an illustrated view of how this cabling should appear.

NOTE: You can make sure that switches and ports are connected as you have them documented with an *nbrStateShow* command. A *topologyShow* command will reveal if you have more than one fibre optic cable between the switches on each site.

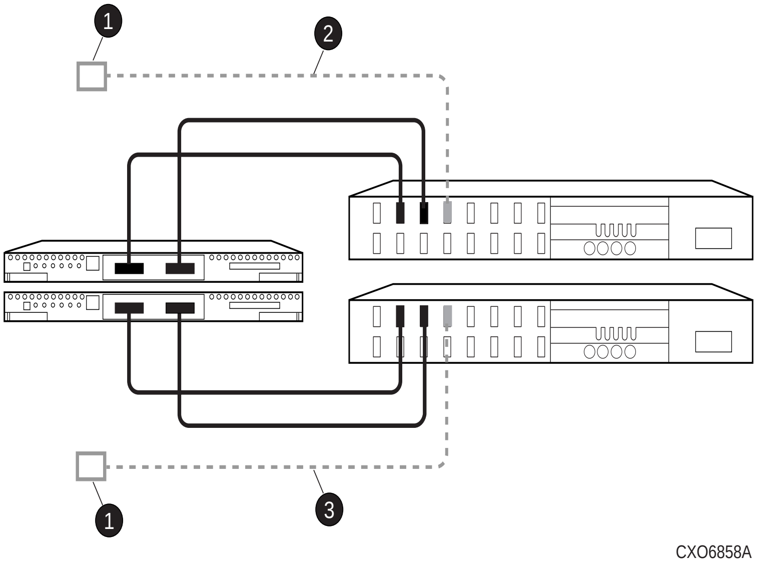


Figure 3–2. Cabling from the Target Site to the Initiator Site

Configure the Host

Install the Host Bus Adapters and Drivers

To run Data Replication Manager, you should have two host bus adapters installed into your host system. If you are installing in a WindowsNT Intel host, refer to the *RAID Array 8000/ESA 12000 Fibre Channel Storage Subsystem for Windows NT Server - Intel Quick Setup Guide* (HSG80 ACS Version 8.4).

NOTE: If you are using WindowsNT, you will need to update the default Topology value. Follow the procedures outlined in the next section.

Update the Topology (Windows NT only)

1. Access REGEDT32.
2. Find DriverSetting with the following sequence:
   - HKEY_LOCAL_MACHINE\SYSTEM
     - Services
       - CurrentControlSet
         - Lp6nds35
           - Parameters
             - Device
               - DriverSettings
3. Change the value of *Topology* in the string to *1*. This will tell the driver to operate in a Fibre Channel switched environment.
4. Exit the Registry Editor.

Install Windows NT (optional)

If you choose to run Windows NT, you will need to install it at this time. Refer to the *RA8000 and ESA12000 HSG80 Solution Software V8.3/V8.4 for WindowsNT Server - Intel Installation Reference Guide* for complete details on this procedure.

Install Secure Path

Verify that your drivers are already started by looking in the *Devices* option of your Control Panel. Verify the servers by looking in the *Services* option in the Control Panel. Make sure that both services listed have an automatic startup and that the HszCheck service is only running during system startup time.

Use the *Secure Path Agent Configuration* to grant access to the client at both the initiator and target sites. This can be found by following these menus:

- Program Files
  - StorageWorks

- SecurePathAgent
    - SecurePathCfg

You can set the password and allow client access via the *Secure Path Agent Configuration*.

> **NOTE:** Compaq recommends that you set both the full and unqualified DNS names as valid, authorized clients.

You are now ready to run Secure Path Manager, which can be found in the *Start/ Programs/StorageWorks/Secure Path Manager* path. Start the application, and specify the server and password that you prefer. Select the “Save Password” box if you would like to use the same password each time you log in.

The StorageWorks Secure Path Manager screen appears, and now you must verify the drives. Go to the disk you want to check, right-click the mouse, and choose *Properties*. You will see the device properties.

Install SWCC (optional)

Detailed information about SWCC can be found in the DIGITAL *StorageWorks Command Console Getting Started Guide*.

Connect Fiber Optic Cables Between the Hosts and the Switches

1. Connect a short-wave, 50 micron fiber optic cable from port 0 of the top switch to the host.
2. Connect the final short-wave, 50 micron fiber optic cable from port 0 of the bottom switch to the host.

> **NOTE:** You may choose any available port to connect your cables to, but you must maintain that identical scheme at the initiator site. Therefore, if port 1 of controller B is connected to port 2 of the bottom switch at the target site, then port 1 of controller B must be connected to port 2 of the bottom switch at the initiator site.

The host is now connected to the target site via the short-wave, 50 micron fiber optic cables. Your cabling should appear as it does in Figure 3–3.

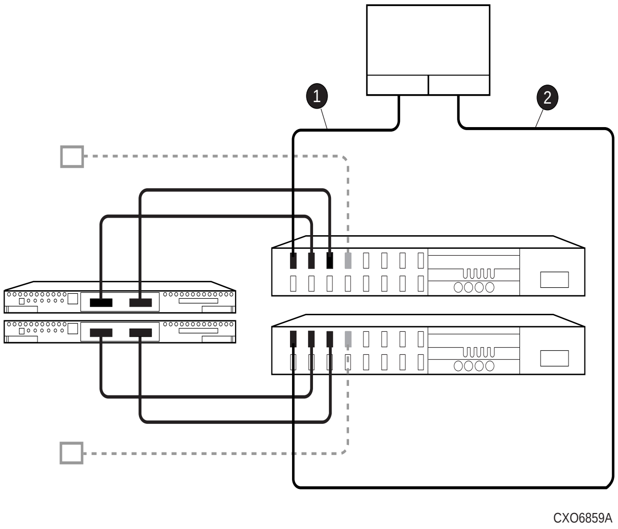


Figure 3–3. Cabling between the Host and the Switches

3. Verify that the connection between the host and the switch has been made by entering this CLI command:

```
SHOW CONNECTIONS
```

NOTE: You can also verify that a connection has been made by looking for the illuminated LED that flashes on the switch ports.

You will see a display similar to the following:

```
Connection                                          Unit
Name       Operating system    Controller  Port    Address    Status   Offset

!NEWCON00        WINNT             THIS       1      210113   offline     0
        HOST_ID=nnnn-nnnn-nnnn-nnnn        ADAPTER_ID=nnnn-nnnn-nnnn-nnnn

!NEWCON01        WINNT             THIS       1      200013   offline     0
        HOST_ID=nnnn-nnnn-nnnn-nnnn        ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
```

Rename the Host Connections

To better identify which hosts you are working with, Compaq recommends that you rename the prompts that are reserved for the host names. This involves changing the !NEWCON prompt to a meaningful host name, according to the host world wide name that you recorded in Chapter 2 and its associated path number. Figure 3–4 is a helpful worksheet to use when renaming your hosts. Fill in the fields accordingly to keep an accurate record of connections and host names.

!NEWCON*xx*	**Worldwide Name**	**Host Name**	**Path Number**

Figure 3–4. Host Renaming Worksheet

When you have completed the worksheet, rename the !NEWCON*xx* prompt using the following CLI commands:

```
RENAME !NEWCONxx TargetHostConnectionNamex
RENAME !NEWCONxx TargetHostConnectionNamey
```

When you have finished renaming your host connections, enter the following command to see your new settings:

```
SHOW CONNECTIONS
```

Configure the Controllers at the Initiator Site

Prior to configuring the controllers at the initiator site, be sure to follow these preparatory steps:

- Identify the world wide name on the host bus adapters. See page 2–2 for instructions on how to locate this name.
- Establish the name that you will assign to the initiator site. This name should be different than the one you assigned to the target.

The first step to getting your DT system up and running involves setting up and configuring the controllers. These tasks are outlined below:

1. Ensure that all BA370 enclosures, Fibre Channel switches, power distribution units (PDUs), and the main power supply are off.
2. Plug all cabinet PDU power cords into the main power receptacles.
3. Be sure that you have a serial connection to each of the controllers.
4. Apply power to the main power source.
5. Turn on all PDUs.
6. Ensure that the switches are powered on but not cabled.
7. Turn on the BA370 cabinets.

   NOTE: When the BA370 cabinets are turned on, the controllers will boot if the PCMCIA cards are already installed. If there are no cards in the controller slots, insert them now, and depress the reset button. Refer to the *HSG80 Array Controller ACS Version 8.4 Configuration and CLI Reference Guide* for complete instructions on how to properly seat the controller cards.
8. Establish a local connection to the controller. Refer to the *HSG80 Array Controller ACS Version 8.4 Maintenance and Service Guide* for instructions.
9. Verify that all controllers are on and functional by looking for the CLI prompt on the maintenance port terminal.

   NOTE: Unless otherwise noted, all operations may be conducted from controller A.

10. Issue the following CLI command:

    SHOW THIS

    You will see a display similar to the following:

```
Controller:
            HSG80 ZG8nnnnnnn Software R0nnP-0, Hardware  E03
            NODE_ID          = nnnn-nnnn-nnnn-nnnn
            ALLOCATION_CLASS = 0
            SCSI_VERSION     = SCSI-2
            Not configured for dual-redundancy
                Controller misconfigured -- other controller present
            Device Port SCSI address 7
            Time: NOT SET
            Command Console LUN is disabled
    Host PORT_1:
            Reported PORT_ID = nnnn-nnnn-nnnn-nnnn
            PORT_1_PROFILE   = PLDA
            PORT_1_TOPOLOGY  = OFFLINE (offline)
    Host PORT_2:
            Reported PORT_ID = nnnn-nnnn-nnnn-nnnn
            PORT_2_PROFILE   = PLDA
            PORT_2_TOPOLOGY  = OFFLINE (offline)
            NOREMOTE_COPY
    Cache:
           512 megabyte write cache, version 0012
           Cache is GOOD
           No unflushed data in cache
            CACHE_FLUSH_TIMER = DEFAULT (10 seconds)
    Mirrored Cache:
            Not enabled
    Battery:
           FULLY CHARGED
            Expires:             WARNING: UNKNOWN EXPIRATION DATE!
           WARNING: AN UNKNOWN NUMBER OF DEEP DISCHARDGES HAVE OCCURRED!
            NOCACHE_UPS
   Controller misconfigured. Type SHOW THIS_CONTROLLER
```

11. Verify that the subsystem world wide name is set. If it is, go to step 15. If the worldwide name has not been assigned to the controller, you will need to obtain the name and set it before proceeding.

    NOTE: The subsystem's worldwide name can be found on a sticker, which is located on top of the frame that houses the controllers, the EMU, the PVA, and the cache modules. If there is no label there, contact your Compaq customer service representative for assistance in obtaining this information. Refer to the *HSG80 Array Controller ACS Version 8.4 Configuration and CLI Reference Guide* for more information on worldwide names.

CAUTION: If you attempt to set the subsystem worldwide name to a name other than the one that came with the subsystem, the data on the subsystem will not be accessible. Never set two subsystems to the same worldwide name, or data corruption will occur.

12. Once the worldwide name has been located, assign it to the controller using the following CLI command:

    ```
    SET THIS NODE_ID=node ID
    ```

    The display should reflect the following:

    ```
    Warning 4000: A restart of this controller is required before all the
          parameters modified will take effect
    %CER--HSG80> --09-FEB-1999 10:07:54-- Restart of this controller required
    Restart of this controller required
    ```

13. Restart the controller using the following CLI command:

    ```
    RESTART THIS
    ```

NOTE: Once you have restarted the controller, you will see a series of %LFL, %CER, and %EVL prompts. These indicate a Last Failure Log, a CLI Event Report, and an Event Log, respectively. For a complete explanation of the event reports, refer to the *HSG80 Array Controller ACS Version 8.4 Maintenance and Service Guide*.

14. Issue a SHOW THIS command to verify that the worldwide name has been set. You should see a display similar to the following:

```
Controller:
            HSG80 ZG8nnnnnnn Software R0nnP-0, Hardware  E03
            NODE_ID          = nnnn-nnnn-nnnn-nnnn
            ALLOCATION_CLASS = 0
            SCSI_VERSION     = SCSI-2
            Not configured for dual-redundancy
                Controller misconfigured -- other controller present
            Device Port SCSI address 7
            Time: NOT SET
            Command Console LUN is disabled
.
.
.
```

15. Check to see what failover mode the controller is in by looking for a configuration message in the display. Use the following CLI command:

```
SHOW THIS
```

a. If the controller is in multiple bus failover mode, go to step 18.

b. If the controller is in transparent mode, issue the following CLI command:

```
SET NOFAILOVER
```

Proceed to step c.

c. If the controllers are not configured for any failover mode, issue the following CLI command:

```
SET MULTIBUS_FAILOVER COPY=THIS_CONTROLLER
```

This command automatically reboots the “other” controller.

You will see a %LFL and %EVL prompt. Refer to the *HSG80 Array Controller ACS Version 8.4 Maintenance and Service Guide* for more details on these reports.

16. To ensure that the settings from step 15 have been applied, enter:

```
SHOW THIS FULL
```

The output will show that the controller have been configured to support multiple bus failover mode:

```
Controller:
            HSG80 ZG8nnnnnnn Software R0nnP-0, Hardware  E03
            NODE_ID          = nnnn-nnnn-nnnn-nnnn
            ALLOCATION_CLASS = 0
            SCSI_VERSION     = SCSI-2
            Configured for MULTIBUS_FAILOVER with ZG8nnnnnnn
                In dual-redundant configuration
            Device Port SCSI address 7
            Time: NOT SET
            Command Console LUN is disabled
.
.
.
```

NOTE: These settings will automatically be applied to controller B. Therefore, it is not necessary to repeat these steps again on controller B.

17. Verify that the settings have been accepted on controller B by using the following CLI command:

    ```
    SHOW OTHER FULL
    ```

18. Change your controller prompts to help you easily identify which component you are working on. Enter the following CLI commands:

    ```
    SET THIS_CONTROLLER PROMPT=
    ```

    ```
    SET OTHER_CONTROLLER PROMPT=
    ```

    NOTE: Be sure to specify a meaningful *InitiatorName*. Do not use “local” and “remote”; these are reserved keywords. The name can be up to eight characters and must be unique to all of your controllers. Follow the naming guidelines as specified in the *HSG80 Array Controller ACS Version 8.4 Configuration and CLI Reference Guide*.

19. If you are not working in a Windows NT environment, proceed to step 23. If you are using Windows NT, check to see if the Command Console LUN (CCL) is disabled. Use the following CLI command

    ```
    SHOW THIS
    ```

20. If the CCL is not disabled, issue the following CLI command:

    ```
    SET THIS NOCOMMAND_CONSOLE_LUN
    ```

21. Verify that the CCL has been disabled by using the following CLI command:

    ```
    SHOW THIS
    ```

    The display will indicate that the CCL has been disabled:

    ```
    Controller:
                HSG80 ZG8nnnnnnn Software R0nnP-0, Hardware  E03
                NODE_ID          = nnnn-nnnn-nnnn-nnnn
                ALLOCATION_CLASS = 0
                SCSI_VERSION     = SCSI-2
                Configured for MULTIBUS_FAILOVER with ZG8nnnnnnn
                    In dual-redundant configuration
                Device Port SCSI address 7
                Time: NOT SET
                Command Console LUN is disabled
    .
    .
    .
    ```

22. Verify that the settings you have established from controller A have been applied to controller B by using the following CLI command:

    ```
    SHOW OTHER
    ```

23. Check to see if mirrored write-back cache is enabled by using the following CLI command:

    ```
    SHOW THIS
    ```

    If it is not enabled, issue the following CLI command:

    ```
    SET THIS_CONTROLLER MIRRORED_CACHE
    ```

    The controllers will reboot after mirrored write-back cache has been set, and you will see %LFL and %EVL displays.

24. After the controllers reboot, issue the following CLI command to confirm that mirrored write-back cache is enabled:

    ```
    SHOW THIS
    ```

Notice that mirrored write-back cache is now set:

```
.
.
.
    Mirrored Cache:
            256 megabyte write cache, version 0012
            Cache is GOOD
            No unflushed data in cache
.
.
.
```

It is not necessary to repeat this step on controller B.

25. Set the fabric topology for each port on both controllers using the following CLI commands:

    NOTE: You will be prompted to restart the controllers after each command, but you do not need to reboot the controllers until all topologies have been set.

    ```
    SET THIS_CONTROLLER PORT_1_TOPOLOGY=FABRIC

    SET THIS_CONTROLLER PORT_2_TOPOLOGY=FABRIC

    SET OTHER_CONTROLLER PORT_1_TOPOLOGY=FABRIC

    SET OTHER_CONTROLLER PORT_2_TOPOLOGY=FABRIC
    ```

26. Restart the controllers (in this order) with the following CLI commands:

    ```
    RESTART OTHER_CONTROLLER

    RESTART THIS_CONTROLLER
    ```

27. To ensure that fabric is up and running, issue the following CLI command:

```
              SHOW THIS
.
.
.
Host PORT_1:
     Reported PORT_ID = nnnn-nnnn-nnnn-nnnn
     PORT_1_PROFILE   = PLDA
     PORT_1_TOPOLOGY  = FABRIC (fabric up)
     Address     =nnnnnn
Host PORT_2:
     Reported PORT_ID = nnnn-nnnn-nnnn-nnnn
     PORT_2_PROFILE   = PLDA
     PORT_2_TOPOLOGY  = FABRIC (fabric up)
     Address     =nnnnnn
     NOREMOTE_COPY
.
.
.
```

28. You are now ready to enable Data Replication Manager. Use the following CLI command:

```
SET THIS_CONTROLLER REMOTE COPY=InitiatorName
```

After you have entered this CLI command, you will see a series of %LFL and %EVL displays, and the controllers will automatically reboot.

29. Use the following CLI command to verify that these settings are in place:

```
              SHOW THIS
.
.
.
Host PORT_2:
            Reported PORT_ID = nnnn-nnnn-nnnn-nnnn
            PORT_2_PROFILE   = PLDA
            PORT_2_TOPOLOGY  = FABRIC (point to point up)
            REMOTE_COPY = TRGT
.
.
.
```

Configure the Storage at the Initiator Site

Devices and StorageSets

Before you can configure the storage for Data Replication Manager, you need to add the disks, create the RAIDsets, and create units. Follow the instructions in the *HSG80 Array Controller ACS Version 8.4 Configuration and CLI Reference Guide*, but note the restrictions listed at the beginning of this chapter.

NOTE: Keep in mind that the initiator site must have the same exact storageset and unit configuration as the target site.

LUNs

Before you can configure the storage at the initiator site, you must first configure the LUNs. Refer to the *HSG80 Array Controller ACS Version 8.4 Configuration and CLI Reference Guide* for detailed information.

Once all of the units and LUNs have been created, you can proceed to the steps below.

1. Disable access on all units with this command:

```
SET Unit DISABLE_ACCESS_PATH=ALL
```

NOTE: Be sure to issue this command for all units.

2. Verify that the access on each unit is set to none by using the following CLI command:

```
SHOW UNIT FULL
```

The display will be similar to the following:

```
LUN                                      Uses             Used by
------------------------------------------------------------------------------

D10                                   DISK1000
  LUN ID:      nnnn-nnnn-nnnn-nnnn-nnnn-nnnn-nnnn-nnnn
  NOIDENTIFIER
  Switches:
    RUN                    NOWRITE_PROTECT        READ_CACHE
    READAHEAD_CACHE        WRITEBACK_CACHE
    MAXIMUM_CACHED_TRANSFER_SIZE = 32
  Access:
    NONE
  State:
    ONLINE to this controller
    Not reserved
    NOPREFERRED_PATH
  Size: nnnnnnnn blocks
  Geometry (C/H/S): ( 7000 / 20 / 254 )
.
.
.
```

3. Distribute the units by setting their preferred path. Use either of the following CLI commands:

```
SET Unit PREFERRED_PATH=THIS_CONTROLLER

SET Unit PREFERRED_PATH=OTHER_CONTROLLER
```

NOTE: The target controller should have the same preferred path that the initiator will have.

Keep the busiest LUNs on different host ports, and remember to reboot the controllers after configuring the LUNs. Otherwise, the preferred path settings will not go into effect.

4. The initiator units will need to allow access to the controllers at the target site. Enable access with this command:

```
SET UnitNumber ENABLE_ACCESS_PATH=(TargetControllerConnectionC,TargetControllerConnectionD)
```

NOTE: *TargetC* and *TargetD* are ports 2 on the controller. Be sure to repeat this command for each *UnitNumber.*

5. Verify that the initiator units have access to the target controller with this CLI command:

   ```
   SHOW REMOTE FULL
   ```

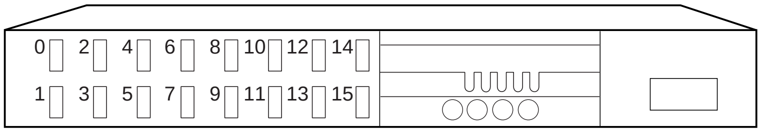
   All remote copy sets should be normalizing.

6. To ensure that your storage settings are in place, use the following CLI command:

   ```
   SHOW STORAGE FULL
   ```

Connect Fiber Optic Cables Between the Controllers and Switches

To better understand which ports you will be instructed to connect the cables to, remember that the port locations on the switch are as follows:



CXO6871A

1. Connect a short-wave, 50 micron fiber optic cable from port 1 of controller A to port 2 of the top Fibre Channel switch.
2. Connect a second short-wave, 50 micron fiber optic cable from port 2 of controller A to port 4 of the top Fibre Channel switch.
3. Connect a third short-wave, 50 micron fiber optic cable from port 1 of controller B to port 2 of the bottom Fibre Channel switch.
4. Connect a fourth short-wave, 50 micron fiber optic cable from port 2 of controller B to port 4 of the bottom Fibre Channel switch.

   NOTE: You should see an illuminated LED on the switch as soon as the cable is inserted. This verifies that there is a good connection.

Figure 3–5 illustrates what your cabling should look like. The numbered callouts reflect the steps that you just completed.

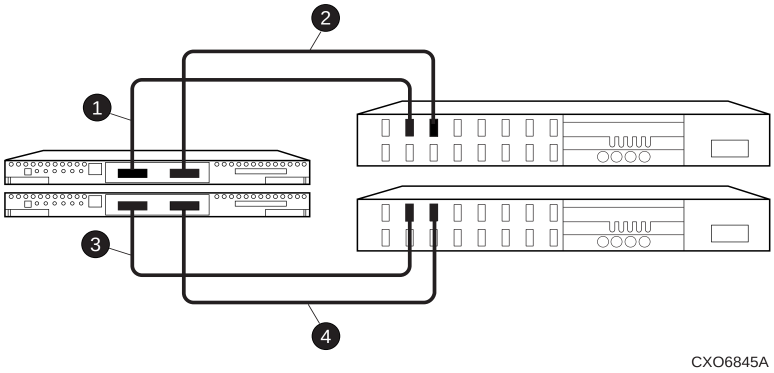


Figure 3–5. Cabling Between the Controllers and Switches

Connect the Initiator Site to the External Fiber Link

1. Locate the connection points at the initiator site that link the initiator site to the target site. Look for either a fiber optic cable connector or a patch panel where you can insert a cable.
2. Connect a long-wave, 9 micron fiber optic cable from port 6 of the top switch to one connection point.
3. Connect another long-wave, 9 micron fiber optic cable from port 6 of the bottom switch to the other connection point.

The initiator site is now physically linked to the target site. See Figure 3–6 for an illustrated view of how this cabling should appear.

> **NOTE:** You can make sure that switches and ports are connected as you have them documented with an *nbrStateShow* command. A *topologyShow* command will reveal if you have more than one fibre optic cable between the switches on each site.

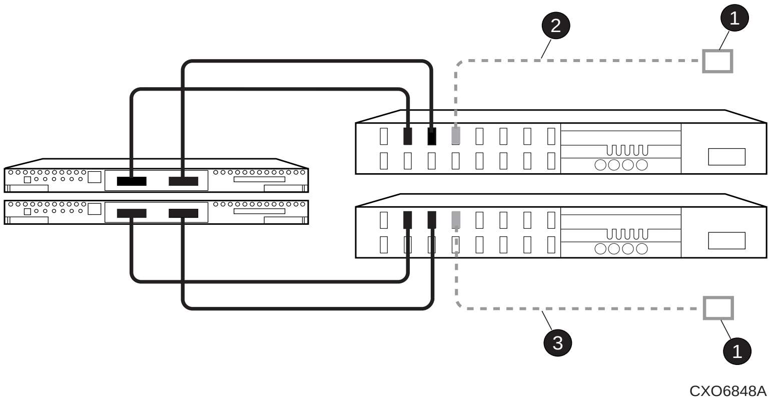


Figure 3–6. Cabling from the Initiator Site to the Target Site

Create Remote Copy Sets

The CLI command below will allow you to create connections between the initiator and target sites. Once these connections are established at the initiator site, a full copy to the target site begins.

Use the following CLI command to create remote copy sets:

```
ADD RemoteCopySetName InitiatorUnit TargetName\UnitName
```

NOTE: It is not necessary to repeat this step at the target site.

You will see %EVL display that includes your remote copy set information:

```
%EVL--Initra > --13-JAN-1946 05:01:56 (time not set)-- Instance Code: 0E010064
  Template: 144.(90)
  Power On Time: 0. Years, 36. Days, 6. Hours, 45. Minutes, 22. Seconds
  Controller Model: HSG80
  Serial Number: ZG8nnnnnnn Hardware Version:  Enn(2B)
  Software Version: R0nnP(FF)
  Informational Report
  Target Controller Board Serial Number: "      ZG8nnnnnnn"
  Initiator WWLID: nnnn-nnnn-nnnn-nnnn-nnnn-nnnn-nnnn-nnnn
  Initiator Node Name: "INITR"
  Initiator Unit Number: n.(nnnnnnnn)
  Target WWLID: nnnn-nnnn-nnnn-nnnn-nnnn-nnnn-nnnn-nnnn
  Target Node Name: "TRGT"
  Target Unit Number: n.(nnnnnnnn)
  Number of Targets: n.(nnnnnnnn)
  Remote Copy Set Name: "RMT0"
  Instance Code: 0E010064
```

Set Failsafe at the Initiator Site (optional)

When failsafe is set, the associated remote copy set must contain at least one initiator member and one target member. If the remote copy set loses a sufficient number of members while failsafe is set, no further I/O will be allowed to this remote copy set, and an error will be returned to the host. This is known as a failsafe locked condition. If you choose to set failsafe, enter the following command:

```
SET RemoteCopySetName ERROR_MODE=FAILSAFE
```

NOTE: When you set failsafe, all remote copy sets must be in a normal or normalizing state. If remote copy sets are copying when you set failsafe, your command will be rejected until the remote copy sets return to normal mode.

To remove the failsafe lock from a remote copy set and resume normal operation, use the following CLI command:

```
SETRemoteCopySetName ERROR_MODE=NORMAL
```

This can also be used for remote copy sets where a DT-safe condition is not required.

NOTE: If you set the error mode to normal while in a failsafe lock condition, the remote copy set is no longer considered DT-safe.

Save Configuration to a Disk

Follow the procedures outlined in the *HSG80 Array Controller ACS Version 8.4 Configuration and CLI Reference Guide* to save your configuration to a disk.

NOTE: If you lose access to all of your data, a site failback is not possible. Therefore, it is imperative that you save your original configuration to a disk and store it in a separate place. If a disaster occurs, you will then be able to access your original information and conduct a successful failback. See Chapter 4 for more information on failback.

Configure the Host

Install the Host Bus Adapters and Drivers

To run Data Replication Manager, you should have two host bus adapters installed into your host system. If you are installing in a WindowsNT Intel host, refer to the *RAID Array 8000/ESA 12000 Fibre Channel Storage Subsystem for Windows NT Server - Intel Quick Setup Guide* (HSG80 ACS Version 8.4).

NOTE: If you are using WindowsNT, you will need to update the default Topology value. Follow the procedures outlined in the next section.

Update the Topology (Windows NT only)

1. Access REGEDT32.
2. Find DriverSetting with the following sequence:
   - HKEY_LOCAL_MACHINE\SYSTEM
     - Services
       - CurrentControlSet
         - Lp6nds35
           - Parameters
             - Device
               - DriverSettings
3. Change the value of *Topology* in the string to *1*. This will tell the driver to operate in a Fibre Channel switched environment.
4. Exit the Registry Editor.

Install Windows NT (optional)

If you choose to run Windows NT, you will need to install it at this time. Refer to the *RA8000 and ESA12000 HSG80 Solution Software V8.3/V8.4 for WindowsNT Server - Intel Installation Reference Guide* for complete details on this procedure.

Install Secure Path

Verify that your drivers are already started by looking in the *Devices* option of your Control Panel. Verify the servers by looking in the *Services* option in the Control Panel. Make sure that both services listed have an automatic startup and that the HszCheck service is only running during system startup time.

Use the *Secure Path Agent Configuration* to grant access to the client at both the initiator and target sites. This can be found by following these menus:

- Program Files
  - StorageWorks
    - SecurePathAgent
      - SecurePathCfg

You can set the password and allow client access via the *Secure Path Agent Configuration*.

> **NOTE:** Compaq recommends that you set both the full and unqualified DNS names as valid, authorized clients.

You are now ready to run Secure Path Manager, which can be found in the *Start/ Programs/StorageWorks/Secure Path Manager* path. Start the application, and specify the server and password that you prefer. Select the "Save Password" box if you would like to use the same password each time you log in.

The StorageWorks Secure Path Manager screen appears, and now you must verify the drives. Go to the disk you want to check, right-click the mouse, and choose *Properties*. You will see the device properties.

Install SWCC (optional)

Detailed information about SWCC can be found in the DIGITAL *StorageWorks Command Console Getting Started Guide*.

Connecting Fibre Optic Cables Between the Hosts and the Switches

1. Connect a short-wave, 50 micron fiber optic cable from port 0 of the top switch to the host.
2. Connect the final short-wave, 50 micron fiber optic cable from port 0 of the bottom switch to the host.

The host is now connected to the initiator site via the short-wave, 50 micron fiber optic cables. Your cabling should appear as it does in Figure 3–7.

> **NOTE:** You may choose any available port to connect your cables to, but you must maintain that identical scheme at the target site. In other words, If port 1 of controller B is connected to port 2 of the bottom switch at the initiator site, then port 1 of controller B must be connected to port 2 of the bottom switch at the target site.

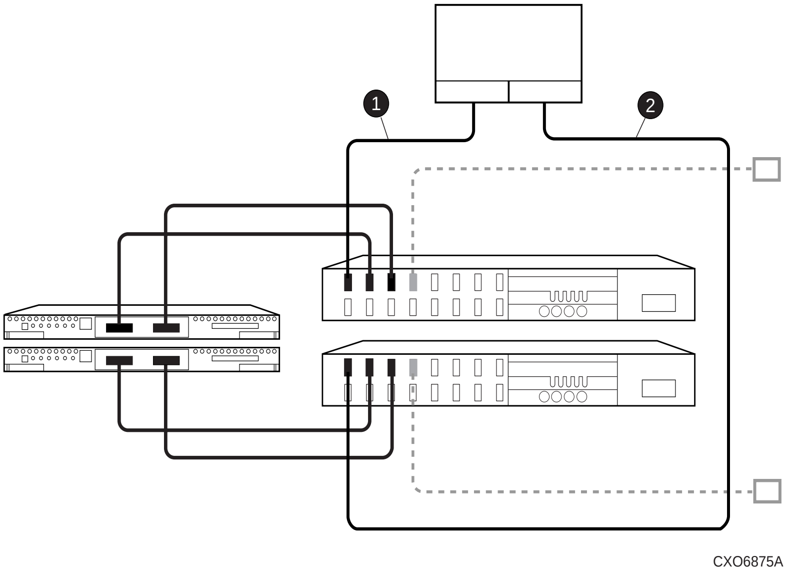


Figure 3–7. Cabling between the Hosts and the Switches

The cabling at each site is now complete. The initiator and target sites should be cabled according to Figure 3–8.

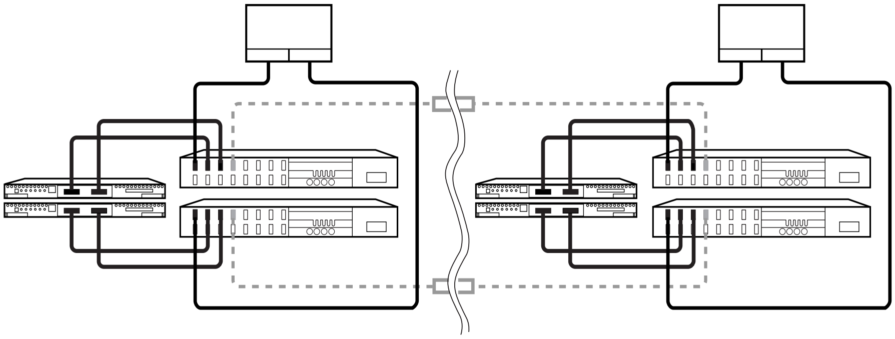


Figure 3–8. Data Replication Manager Cabling at Initiator and Target Sites

3. Verify that the connection between the host and the switch has been made by entering this CLI command:

```
SHOW CONNECTIONS
```

NOTE: You can also verify that a connection has been made by looking for the illuminated LED that flashes on the switch ports.

You will see a display similar to the following:

```
Connection                                           Unit
Name      Operating system    Controller    Port    Address    Status   Offset

!NEWCON00         WINNT             THIS       1      210013   offline    0
       HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn

!NEWCON01         WINNT             THIS       1      200113   offline    0
       HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn

TRGTA          PPRC_TARGET         THIS       2                offline    0
       HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn

TRGTB          PPRC_TARGET        OTHER      2                 offline    0
       HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn

TRGTC         PPRC_INITIATOR       THIS       2                offline    0
       HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn

TRGTD         PPRC_INITIATOR       OTHER      2                offline    0
       HOST_ID=nnnn-nnnn-nnnn-nnnn ADAPTER_ID=nnnn-nnnn-nnnn-nnnn
```

Rename the Host Connections

To better identify which hosts you are working with, Compaq recommends that you rename the prompts that are reserved for the host names. This involves changing the !NEWCON prompt to a meaningful host name, according to the host world wide name that you recorded in Chapter 2 and its associated path number. Figure 3–4 is a helpful worksheet to use when renaming your hosts. Fill in the fields accordingly to keep an accurate record of connections and host names.

!NEWCON*xx*	Worldwide Name	Host Name	Path Number

Figure 3–9. Host Renaming Worksheet

When you have completed the worksheet, rename the !NEWCON*xx* prompt using the following CLI commands:

```
RENAME !NEWCONxx InitiatorHostConnectionNamex
RENAME !NEWCONxx InitiatorHostConnectionNamey
```

When you have finished renaming your host connections, enter the following command to see your new settings:

```
SHOW CONNECTIONS
```

Enable Access to the Hosts

The initiator units will need to have access to the hosts. Enable access with this command:

```
SET Unit ENABLE_ACCESS_PATH=(InitiatorHostConnectionNamex,InitiatorHostConnectionNamey)
```

> **NOTE:** Keep in mind that there should be two paths per host. You will need to repeat this sequence for each host. Be sure to reboot the host after you have enabled access to the hosts.

Verify System Operation

Verify subsystem configuration by issuing these commands from the initiator:

```
SHOW STORAGESET FULL
SHOW REMOTE_SET FULL
SHOW UNIT FULL
```

You will see a display that shows all the assigned remote copy sets and their characteristics. Verify that all storage is available. It is recommended that you save the displayed output so the operator can recreate this configuration by entering the appropriate commands should a recreation of the configuration need to occur. See page 3–37 for more information on saving your configuration.

After the DT storage has been configured, the initiator and target site hosts can be rebooted. The NTDETECT mechanism will recognize all the new units created as individual disks at the initiator site. At this time, the storage units will only be accessible from the initiator site.

You are now ready to use the Disk Administrator to create partitions, format, and assign drive letters on the newly created storage. Once the storage has been configured with Disk Administrator, you need to save this configuration to a floppy for use during a failover or failback condition. To create a saved configuration from the Disk Administrator, perform the following steps:

1. Open Partition and select Configuration.
2. Select Save and insert a floppy as requested.

NOTE: It is recommended that two copies of the saved configuration be created and maintained at both the initiator and target sites. This data will be used to restore a known configuration in the event of a site failover or failback.

Install Cluster Server for Windows NT (optional)

Windows NT Fibre Channel cluster software enables two host servers to share a Fibre Channel storage subsystem through a Fibre Channel switch. If a failure on the server occurs, the cluster software detects that failure, and a failover is initiated. The failed components can be warm-swapped or serviced while the functioning components remain active. This process requires minimal downtime and ensures high availability of data.

If you are using Windows NT and wish to run the cluster option, you can safely install it now. Refer to the *Compaq Storageworks RAID Array8000/ESA12000 Fibre Channel Cluster Solutions for Windows NT Installation Guide*.

Chapter 4
Managing and Operating a Data Replication Manager Solution

This chapter describes how to manage and operate your Data Replication Manager solution.

Managing Data Replication Manager

The procedures below outline how to power on and power off the storage subsystem after it has been configured.

Power Up (after configuration)

> ⚠ **CAUTION:** Compaq recommends that you power up the controllers and switches at the target site before applying power to the initiator site. Powering up in the wrong sequence may cause incorrect configurations.

Power up the system in the following order:

1. From the target site, ensure that all BA370 enclosures, switches, and cabinet power distribution units (PDU) have their power switches in the OFF position.
2. Apply power to all PDUs.
3. Turn on the BA370 power switches for the cabinets at the target site.
4. Make sure that all controllers are up and functional.
5. Apply power to all switches.
6. Repeat steps 1 to 5 at the initiator site.

Power Down

1. From the initiator site, issue the following CLI commands (in this order):

   ```
   SHUTDOWN OTHER
   SHUTDOWN THIS
   ```

2. Turn off the Fibre Channel switch.
3. Turn off the power to the BA370 enclosure.
4. Turn off the PDUs.
5. Repeat steps 1 to 4 at the target site.

Failover

If the initiator site is no longer available, you must decide whether or not to perform a site failover. This will enable the target site to assume the role of the initiator and access data until the problem is resolved. Transferring control of system operation to the target site ensures that there will be minimal interruption in data access after a failure.

> **NOTE:** If you decide to perform a failover, keep in mind that *all* components must be failed over. Therefore, if only one component fails, fixing that single component may be preferable to performing a complete failover.

Table 4–1 outlines the scenarios that may call for a failover and those that may not.

Table 4–1 Failover Scenarios

When to Failover	When Not to Failover (recommended)
■ Both controllers fail ■ Power failure at the initiator site ■ Both host adapters fail ■ Both initiator switches fail ■ Disaster (flooding, fire, earthquake, terrorism, etc.) that disables access to the subsystems) ■ Scheduled event that will prevent computing from the initiator site	■ Failed Switch ■ Fiber optic cable malfunction ■ Single controller fails ■ Single storageset fails ■ Single disk fails
If one host in a multi-host environment fails, you must decide whether or not a failover is the best course of action.	

To perform a failover to the target site, follow the procedures below. It is important to verify that all components at the target site are operational before you begin the failover.

CAUTION: Be sure to follow these steps accurately and completely, or you will incur data loss and extended down time.

From the Initiator Site

1. If the initiator site is still accessible, and the operating system is still up and running, shut it down, and power off the hosts.
2. If the controllers at the initiator site are still functioning, issue the following CLI command:

   ```
   SET Unit DISABLE=(InitiatorHostNamex,InitiatorHostNamey)
   ```

   This will prevent the local server from accessing the local storage subsystems.

   NOTE: If you have multiple hosts, each host will have two connections. Be sure to issue this command for each host connection, but do not delete the remote copy sets.

   Each unit should still have access enabled to the target controllers. You should see four paths in the Access field of the display.
3. Shutdown the initiator HSG80 controllers (in this order) with the following CLI commands:

   ```
   SHUTDOWN_OTHER_CONTROLLER
   SHUTDOWN_THIS_CONTROLLER
   ```

From the Target Site

1. Turn off access to the initiator site by disabling the initiator's C and D connections on each remote unit. This will force the initiator site into a Failsafe lock condition and disable all I/O from the initiator host. Use the following CLI command:

   ```
   SET Unit DISABLE=(InitiatorControllerConnectionC,InitiatorControllerConnectionD)
   ```

2. At the target site, you will need to prevent the initiator from resuming its role if it is restored. Use the following CLI command for each remote copy set (maximum of eight per subsystem):

   ```
   SITE_FAILOVER InitiatorControllerRemoteCopyName\remote_copy_set_name
   ```

   NOTE: Be sure to note which controller you are performing the failover from. You will need to know this if you decide to conduct a failback.

   You will see a %EVL display on your terminal.

3. Give the target site hosts access to the units in its storage subsystems with this command:

   ```
   SET Unit ENABLE=(TargetHostConnectionNamex,TargetHostConnectionNamey)
   ```

   If you do not recall the target host name, use the SHOW CONNECTION command.

   NOTE: You will see a warning message stating that access paths are enabled. At this time, there is no need to disable the access path because the initiator site may be restored.

4. To verify that all of these steps have been completed successfully, issue this CLI command:

   ```
   SHOW REMOTE_COPY_SETS FULL
   ```

   This will give you a list of remote copy sets. Be sure that the units you see are the ones from the target site and not the initiator units.

5. To verify that the target host can connect to the LUNs, use this command:

   ```
   SHOW UNIT FULL
   ```

   In the Access field of the display, all units should show that the target hosts are enabled.

   NOTE: When failing over, it is important to note whether or not the target site has an enabled configuration. If you are running Microsoft Cluster Server, Cluster will not recognize the new units from the original initiator site until you add them. Therefore, you must uninstall Cluster Server, reboot the hosts, configure the new units, reinstall Cluster Server, and proceed with the configurations on both hosts.

6. At the target site, reboot the server, and log in as *Administrator.* You should be able to see all of the drives in *My Computer.*

   NOTE: Even though the target site now acts as the initiator, it is still referred to as the target site.

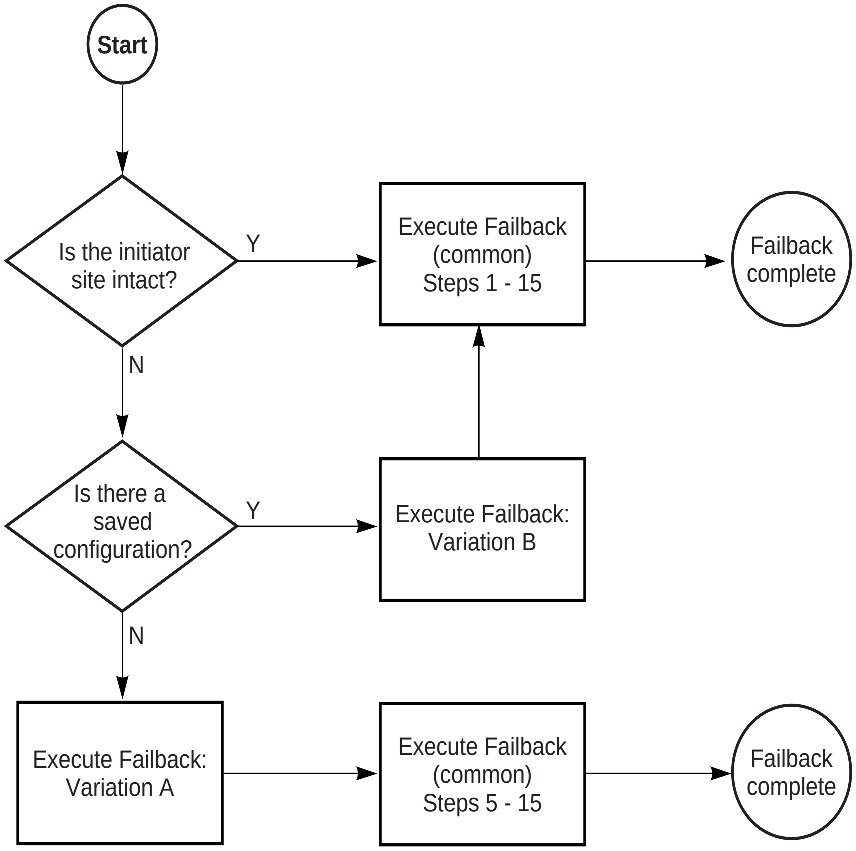
Failback

When the new initiator site has been established or the original one has been restored, site operation can resume there after a failback procedure has been performed. This involves synchronizing both the initiator and target subsystems so that operation can be returned to the initiator with minimal downtime. Verify that all components at both sites are operational before performing a failback.

The failback sequence is a scheduled event based upon the configuration at the failback site. The HSG80 array controller requires that a viable dual redundant subsystem be available before a failback can take place. Failback to a single controller configuration is not supported.

The following sections detail the procedures that will enable you to perform various site failbacks. It is important to understand which failback procedure is appropriate for certain disasters. Refer to the following paragraphs for a description of each failback procedure and which is most appropriate for your situation.

The following flowchart will help you to understand which failback procedure you should refer to before performing a site failback:


Start
Is the initiator site intact?
Y
N
Execute Failback (common) Steps 1 - 15
Failback complete
Is there a saved configuration?
Y
N
Execute Failback: Variation B
Execute Failback: Variation A
Execute Failback (common) Steps 5 - 15
Failback complete

CXO6886A

Failback (common)

A common failback is the foundation for all failback procedures. When the initiator site is still intact, a common site failback is the designated course of action. All failback procedures, however, will incorporate some element of this common procedure.

From the Initiator Site

1. Disable access to all of the units with the following CLI command:

   ```
   SET UnitNumber DISABLE=ALL
   ```

   This command needs to be issued to all units that involve remote copy sets. A failsafe lock condition will be triggered if the initiator host is still up and accessing the units.

2. Shut down the initiator host if it is still up and running.
3. Reset the error modes on the remote copy sets by using the following CLI command:

   ```
   SET RemoteCopySetName ERROR=NORMAL
   ```

4. Delete the remote copy set on the initiator by using the following CLI command:

   ```
   DELETE RemoteCopySetName
   ```

5. Repeat steps 3 and 4 for all remote copy sets.
6. Issue the following CLI command:

   ```
   SET UnitNumber ENABLE=(TargetC,TargetD)
   ```

   Reenter this command to all units that involve remote copy sets.

From the Target Site

7. Enter the following CLI command:

   ```
   SET UnitNumber ENABLE=(InitiatorNameC,InitiatorNameD)
   ```

   Repeat this step for all units that involve remote copy sets.

8. Add the units to the remote copy sets with the following CLI command:

```
SET RemoteCopySetName ADD=InitiatorName\ UnitNumber
```

IMPORTANT: You must wait for normalization on all units to complete before you can proceed.

From the Initiator Site

9. Issue the following CLI command:

```
ADD REMOTE RemoteCopySetName UnitNumber
```

From the Target Site

10. Shut down the target host.
11. Disable access to the target units by using the following CLI command:

```
SET UnitNumber DISABLE=(TargetHostConnectionNamex,TargetHostConnectionNamey)
```

12. Reassign the remote copy sets to the unit numbers using the following CLI command:

```
SET RemoteCopySetName INITIATOR=InitiatorName\UnitNumber
```

From the Initiator Site

13. Enable access to the units by using the following CLI command:

```
SET UnitNumber ENABLE=(InitiatorHostConnectionNamex,InitiatorHostConnectionNamey)
```

14. Set failsafe by using the following CLI command:

```
SET RemoteCopySetName ERROR=FAILSAFE
```

15. Boot the initiator host.

Failback: Variation A

There are times when a common failback is not sufficient to restore your original configuration. Situations may arise when there is no saved configuration and the initiator site is not intact. This could mean that your Nonvolatile Random Access Memory (NVRAM) is destroyed, you are working with all new hardware that is not configured, or you have decided to failback to a third site.

If you have encountered any one of the above scenarios, follow the procedures for Variation A below:

From the Initiator Site

1. Manually reconfigure the controllers, but do not recreate the original remote copy sets. Refer to Chapter 3, pages 3–23 to 3–35.
2. Disable access to all units by issuing the following CLI command:

   ```
   SET UnitNumber DISABLE=ALL
   ```

3. Delete the connections to the controllers at the initiator site using the following CLI command:

   ```
   DELETE InitiatorNameA,InitiatorNameB,InitiatorNameC,InitiatorNameD
   ```

   The only access on the target units should be from the hosts.
4. Issue the following CLI commandS:

   ```
   ADD REMOTE RCS199 D199 InitiatorName\D199
   ```

   ```
   ADD REMOTE RCS199 D199 TargetName\D199
   ```

   NOTE: These commands will fail, but they create and name the connections appropriately.
5. At this point, you will need to perform the last portion of the common failback procedure, beginning with step 6 on page 4–9.

Failback: Variation B

Use the following procedure when you have encountered a situation where your initiator site is no longer intact and you have a configuration saved on a disk. This includes situations where the Nonvolatile RAM on the initiator controller is inconsistent with the original configuration or all new hardware is in place. Variation B is also recommended for situations that involve a new site entirely.

NOTE: The worldwide id on the new hardware will be the worldwide of the original initiator. This is an exception to the previous warning that appeared on page 3–8.

CAUTION: If the original equipment is still functional, be sure that it is never configured with the newly restored worldwide id. In this situation, data loss could occur as a result of duplicate worldwide ids in use.

From the Initiator Site

1. Place the disk containing the saved configuration into an available slot in the storage cabinet.
2. With only one of the controllers booted, issue the following CLI command:

```
CONFIGURATION RESTORE
```

3. Boot the second controller.
4. From the *same* controller that you restored the configuration to, enable multiple bus failover by using the following CLI command:

```
SET MULTIBUS COPY=THIS
```

5. Set mirrored cache with the following CLI command:

```
SET THIS MIRRORED_CACHE
```

6. Return to step 1 on page 4–9, and perform the common failback procedure in its entirety.

Chapter 5
Troubleshooting

This chapter describes possible failure modes of a Data Replication Manager solution. Isolation of errors and detailed error analysis require a complete understanding of how the storage subsystem operates. While it is not possible to document every error and failure condition, key failures of the Data Replication Manager subsystem and its components are discussed.

Troubleshooting information on specific Data Replication Manager components can also be found in their respective user manuals.

HSG80 Array Controller Operating Characteristics

The HSG80array controller has certain characteristics that may become evident when used in a Data Replication Manager solution. The following sections will help you understand these characteristics and educate you on how to respond to them.

Forced Errors Detected During Copy

A forced error is a data bit indicating that a corresponding logical data block contains unrecoverable data. If a read request from the initiator to the target encounters a forced error during a full copy, then the data in that block will be copied to the target and marked with a forced error. These forced errors are then reported to the host and reappear each time the block is read. The file containing the forced error qualifier should be restored from a known good backup.

Refer to the *HSG80 Array Controller ACS Version 8.4 Maintenance and Service Guide* for complete details on how to recover from a forced error situation.

Read Errors Detected During Full Copy

During normal operation, an unrecoverable error is reported to the host, the offending block is revectored, and the new block is marked with a forced error. During a full copy, however, the handling is slightly different because the block that is unrecoverable may not be within normal file system space. Therefore, the controller will terminate the copy and report the event.

Unrecoverable read errors on the source member will terminate the copy and send a fault management report to the host. Refer to the *HSG80 Array Controller ACS Version 8.4 Configuration and CLI Reference Guide* for more information on how to interpret these logs.

Dual Redundancy During Failback

The failback sequence is a scheduled event based upon the configuration at the failback site. The HSG80 array controller requires that a viable dual redundant subsystem be available before a failback can take place. Failback to a single controller configuration is not supported.

Failsafe Lock Management

If failsafe mode is set and a write I/O fails to the target member, a remote copy set is placed in failsafe locked condition. When the initiating controller detects a failed I/O to the target, it will remove the target from the remote copy set and place the unit in failsafe lock condition. When this happens, a serious event may have occurred, and recovery actions are necessary. You may choose to reset the error mode to normal and continue processing at the initiator data center, or you may want to execute a site failover to begin processing at an alternate location.

When the condition that caused the I/O to fail is corrected, the target member can be added back to the remote copy set, and a full copy from the initiator to the target will occur. Refer to Chapter 4 for more information.

Link Failure Management

When an initiator controller detects that the link to its target controller is unavailable, the initiating controller will restart. This causes all remote copy sets on the initiating controller to failover to its dual redundant partner controller. The restart of the initiator controller is an intended action and is not an indicator of a defective controller.

Remote Copy Set Member Failures

While most remote copy set members will be based on protected storage in the unlikely event of a remote copy set member failure, the following operating characteristics should be understood:

- If a remote copy set target member fails, a write issued to that remote copy set will cause a write failure at the target. The target member will be removed, and the remote copy set will be put in failsafe lock condition. If you wish to continue operation at the initiator site, be sure to change the remote copy set error mode to normal before proceeding.
- If a remote copy set member at the initiator fails, the unit will become unavailable to the host. The target member of the remote copy set is not read and write accessible through the initiator controller. Recovery from this condition requires a failover to the target site.

Remote Copy Set Worldwide LUN ID

Remote copy sets are assigned a unique worldwide LUN id (WWLID) that represents their specific LUN. The controller identifies a remote copy set by its WWLID and presents it to the target when a failover is executed for that unit. If the remote copy set is failed over to a target site, its WWLID will be transferred with that unit, even though it may not be consistent with the controller’s worldwide id or the ids of the other units presented on the new controller. The remote copy set will not assume a new WWLID, regardless of those that appear at the target site.

Component Failures

The service and maintenance of a Data Replication Manager solution is based on failure of subsystem components. When a component fails, you must determine the cause of the failure, the most appropriate workaround to eliminate down time, and the best course of action to resolve the problem.

Failure Notification

It is important to understand the operation of the DT subsystem and the individual component error logging methods that are used to analyze failures on a DT subsystem. Each component within the DT subsystem provides error and failure information specific to the function being performed. The array controllers maintain and log specific information relevant to the operation and the devices connected to both the host ports and device ports of the controllers. Events, errors, and failures related to a DT subsystem are provided to the host. Information is available from the HSG80 controller via the serial maintenance port.

With Data Replication Manager, fault management events that occur on the target controllers are “passed through” and reported on the initiator controllers. The initiator then reports these events to the host via Template 90. See the *HSG80 Array Controller ACS Version 8.4 Maintenance and Service Guide* for more information.

HSG80 Array Controller Failure

The HSG80 array controller provides event and error reporting via the controller’s serial maintenance port. To help capture random disk errors associated with the controllers, a terminal can be connected to this maintenance port. For a complete explanation and examples of these codes, see the *HSG80 Array Controller ACS Version 8.4 Maintenance and Service Guide*.

SWCC Failure

SWCC notifies the user of any component loss in the system via an active SWCC Client Graphical User Interface (GUI). This GUI window on the command console monitor is a graphical representation of the controllers and their physical and logical storage elements. SWCC periodically queries the controllers for status. Clients connected to the GUI *.ini* file will be notified via the GUI screen of any changes in status. The user is able to manipulate controllers and storage through the GUI and intervene in the DT process when there is a problem.

Refer to the *StorageWorks Command Console Getting Started Guide* and the on-line users help for more information.

Failure of One Member in a Dual Redundant Controller Pair

Each of the controller pairs can lose a single member to failure. When this happens, a normal controller failover occurs automatically, and the preferred devices will automatically be moved to the remaining controller. A decrease in I/O speed may occur. The faulty controller must be replaced using conventional controller troubleshooting techniques.

NOTE: It is not possible to set up a DT configuration unless both controllers are operational.

Failure of Both Fiber Optic Cables or Switch

If you are operating in failsafe mode and both links between the initiator and target sites are lost, the target site will be removed from all remote copy sets, and all I/O to the remote copy sets will cease. If you are operating in normal mode, then I/O will continue through the initiator host, and the target will still be removed.

If you lose the fiber optic cable connection of a switch at either site, refer to Figure 5–1 for information on how to resolve the problem.

Failure of Network

If the initiator and target sites become partitioned, then failover and failback operations are impossible. These problems must be resolved before normal operations can continue.

Failure Modes of a DT System in Normal Operation

Table 5–1 details the failure modes of a DT system operating in normal mode. While this table concentrates on the major failure possibilities, keep in mind that there are several other combinations that may occur. In most cases, when there is a loss of a major component, a failover is necessary to continue operation.

Table 5–1 Failure Modes of a DT System with Normal Operation

Initiator Host	**Target Host**	**Initiator Switch A**	**Target Switch B**	**Target Switch A**	**Target Switch B**	**Initiator Controller A**	**Initiator Controller B**	**Target Controller A**	**Target Controller B**	**Failure Mode** *Loss of:*	**Action**
X										Applications	Failover; Repair host
	X									Remote host	Repair Host
X	X									Both sites	Failover not possible; Repair Hosts
		X								Data path	Repair Switch
			X							Data path	Repair Switch
				X						Data path	Repair Switch
					X					Data path	Repair Switch
		X	X							Data access	Failover; Repair switches
				X	X					Remote copy set targets	Repair switches; Target member must incur a full copy
		X		X						Data path	Repair Switches

Table 5–1 Failure Modes of a DT System with Normal Operation (Continued)

Initiator Host	Target Host	Initiator Switch A	Target Switch B	Target Switch A	Target Switch B	Initiator Controller A	Initiator Controller B	Target Controller A	Target Controller B	Failure Mode *Loss of:*	Action
						X				Data path	Repair Controller
							X			Data path	Repair Controller
								X		Data path	Repair Controller
									X	Data path	Repair Controller
						X	X			Data access	Failover
								X	X	Remote copy set targets	Repair controllers; Normalize remote copy sets
						X		X		Data path	Repair controllers

Failure at Target Site after Failover

After a failover has occurred, failures at the target site are detected the same as in a non-disaster tolerant state. Table 4-1 shows the possible failure modes at the target site, assuming that the initiator site is not available to failback to.

Table 5–2 Target Site DT Failure Modes After Failover

Target Host	Target Top Switch	Target Bottom Switch	Target Controller A	Target Controller B	Failure Mode	Action
X					Loss of remote site	Repair host
	X				Loss of data path	Repair switch
		X			Loss of data path	Repair switch
	X	X			Loss of data access	Repair switches
			X		Loss of data path	Repair controller
				X	Loss of data path	Repair controller
			X	X	Loss of data access	Repair controllers

Index