

SANworks by Compaq

Data Replication Manager
HSG80 ACS Version 8.6-4P
Failover/Failback Procedures Guide

Part Number: AA-RPJ0C-TE

Third Edition (February 2002)

Product Version: ACS Version 8.6-4P

This Procedures Guide provides a general description of *SANworks*[™] Data Replication Manager by Compaq and introduces the concepts of failover and failback. It provides specific and detailed procedures for performing failover and failback, and for resuming operations after special situations. It also provides troubleshooting help for failover and failback issues.

COMPAQ

© 2002 Compaq Information Technologies Group, L.P.

Compaq, the Compaq logo, SANworks, StorageWorks, Tru64, and OpenVMS are trademarks of Compaq Information Technologies Group, L.P. in the U.S. and/or other countries.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the U.S. and/or other countries.

UNIX is a trademark of The Open Group in the U.S. and/or other countries.

All other product names mentioned herein may be trademarks of their respective companies.

Confidential computer software. Valid license from Compaq required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Compaq shall not be liable for technical or editorial errors or omissions contained herein. The information is provided "as is" without warranty of any kind and is subject to change without notice. The warranties for Compaq products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

Compaq service tool software, including associated documentation, is the property of and contains confidential technology of Compaq Computer Corporation or its affiliates. Service customer is hereby licensed to use the software only for activities directly relating to the delivery of, and only during the term of, the applicable services delivered by Compaq or its authorized service provider. Customer may not modify or reverse engineer, remove, or transfer the software or make the software or any resultant diagnosis or system management data available to other parties without Compaq's or its authorized service provider's consent. Upon termination of the services, customer will, at Compaq's or its service provider's option, destroy or return the software and associated documentation in its possession.

Printed in the U.S.A.

Data Replication Manager HSG80 ACS Version 8.6-4P Failover/Failback Procedures Guide

Third Edition (February 2002)

Part Number: AA-RPJ0C-TE

Contents

About this Guide

What's New	ix
Intended Audience	ix
Related Documentation	x
Software and Firmware Revision Levels	xi
Prerequisites	xii
Document Conventions	xii
Symbols in Text	xii
Symbols on Equipment	xiii
Rack Stability	xiv
Getting Help	xiv
Compaq Technical Support	xiv
Compaq Website	xv
Compaq Authorized Reseller	xv

1 Introduction to Failover/Failback

Data Replication Manager Overview	1-2
Peer-to-Peer Remote Copy Function	1-2
Hardware Redundancy	1-2
Failover and Failback	1-3
Failover	1-4
Failback	1-6
Failsafe-Locked and Normal Modes	1-6
Possible Event Scenarios	1-7
Unplanned Site Failover with Full Failback	1-7
Unplanned Loss of Target While in Failsafe Mode	1-7
Unplanned Loss of Target While in Normal Mode	1-7
Short Duration Initiator Site Maintenance	1-8
Resumption of Replication After Short Planned Loss of Target	1-8
Extended Duration Initiator Site Maintenance	1-8

Resumption of Replication After Extended Planned Loss of Target	1–8
Unplanned Site Failover Due to Disaster at Initiator	1–9
Planned Role Reversal	1–9
Recovery from Disaster During Planned Role Reversal	1–9
Summary of Procedure Choices	1–9
Planned System Power Up or Power Down	1–11
Using Scripts to Automate Failover and Failback Procedures	1–11
Overview	1–12
Requirements	1–12
How Scripts Work	1–12
2 Unplanned Site Failover with Full Failback Procedure	
Unplanned Failover	2–2
Target Site Failover Procedure	2–2
Full Failback	2–12
Initiator Site Preparation Procedure	2–12
Target Site Copy Data Procedure	2–17
Initiator Site Return Control Procedure	2–21
Target Site Restore Procedure	2–22
Initiator Site Restoration of Target Connections Procedure	2–24
3 Resumption of Operations After Unplanned Loss of Target Site Procedure (Failsafe Mode)	
Verification of Lost Connections Procedure	3–2
Resumption of Host Access to Remote Copy Sets Procedure	3–3
Resumption of Operations and Return to Failsafe Mode Procedure	3–4
4 Resumption of Operations After Unplanned Loss of Target Site Procedure (Normal Mode)	
Verification of Lost Connections Procedure	4–2
Resumption of Host Access to Remote Copy Sets Procedure	4–2
Verification of Resumption of Operations Procedure	4–4
5 Short Planned Site Failover with Fast Failback Procedure	
Power Up and Power Down	5–1
Planned Site Failover	5–2
Initiator Site Preparation Procedure	5–2
Target Site Failover Procedure	5–6

Create a Log Unit	5–9
Create Association Sets and Assign a Log Unit	5–11
Target Host Setup Procedure	5–12
Fast Failback	5–19
Target Site Failback Procedure	5–20
Initiator Site Cleanup Procedure	5–22
6 Resumption of Replication After Short Planned Loss of Target Procedure	
Procedure for Planned Loss of Target During Short Maintenance Period	6–1
Suspend Remote Copy Sets for Target Site Shutdown	6–2
Target Site Shutdown	6–6
Resume Remote Copy Sets When Target Site Is Back Up	6–7
7 Extended Planned Site Failover With Full Failback Procedure	
Planned Site Failover	7–2
Initiator Site Preparation Procedure	7–2
Target Site Failover Procedure	7–6
Target Host Setup Procedure	7–11
Maintenance Completion	7–16
Initiator Site Preparation Procedure	7–16
Target Site Copy Data Procedure	7–18
Maintenance Failback	7–20
Continuation of Target Site Copy Data Procedure	7–20
Initiator Site Return Control Procedure	7–21
Target Site Restore Procedure	7–23
Initiator Site Restoration of Target Connections Procedure	7–24
8 Resumption of Replication After Extended Planned Loss of Target Procedure (Failsafe Mode)	
Prepare Remote Copy Sets	8–2
Target Site Availability	8–4
Resume Remote Copy Set Operation	8–4
9 Unplanned Site Failover with Failback to New Hardware Procedure	
Unplanned Failover	9–2
Target Site Failover Procedure	9–2
New Hardware Failback	9–13

Initiator Site Preparation Procedure	9–13
Target Site Preparation Procedure	9–22
Initiator Site Connections Procedure	9–26
Target Site Copy Data Procedure	9–28
Initiator Site Return Control Procedure	9–31
Target Site Restore Procedure	9–34
Initiator Site Restoration of Target Connections Procedure	9–36

10 Planned Site Role Reversal Procedure

Role Reversal Failover	10–1
Initiator Site Preparation Procedure	10–2
Target Site Failover Procedure	10–6
Target Host Setup Procedure	10–10
Role Reversal Failback	10–16
Target Site Failback Procedure	10–16
Initiator Site Cleanup Procedure	10–18

11 Disaster Recovery After Role Reversal Procedure

Role Reversal Unplanned Failback	11–1
Initiator Site Preparation Procedure	11–2
Target Site Cleanup Procedure	11–5
Initiator Site Cleanup Procedure	11–6

12 Troubleshooting

HSG80 Array Controller Operating Characteristics	12–2
Forced Errors Detected During Copy	12–2
Read Errors Detected During Full Copy	12–2
Dual Redundancy During Failback	12–2
Failsafe Lock Management	12–3
Link Failure Management	12–3
Remote Copy Set Member Failures	12–3
Remote Copy Set World Wide LUN ID	12–4
Write History Logging	12–4
Component Failures	12–4
Failure Notification	12–4
SWCC Failure	12–5
Failure of One Member in a Dual Redundant Controller Pair	12–5
Failure Modes of a DT System in Normal Operation	12–6

Failure at Target Site After Failover	12-7
Confirmation Message Instance Codes	12-8

A Status Comparison

Target Site Terminal Emulator Session	A-1
Issuing SHOW Commands	A-1

B DRM Power Up and Power Down

Power Up Data Replication Manager Systems	B-1
Target Site Power Up Procedure	B-1
Initiator Site Power Up Procedure.	B-1
Power Down DRM Systems	B-2
Initiator Site Power Down Procedure	B-2
Target Site Power Down Procedure	B-2

C Creating a Log Unit and Association Sets

Create a Log Unit.	C-1
Create Association Sets and Assign a Log Unit.	C-2

Glossary

Index

Figures

1-1 Basic Data Replication Manager configuration	1-3
------------------------------------------------------------	-----

Tables

1 Document Conventions.	xii
1-1 When and When Not to Failover	1-5
1-2 Procedure Choices.	1-10
12-1 Failure Modes of a DT System with Normal Operation.	12-6
12-2 Target Site DT Failure Modes After Failover.	12-7
12-3 Instance Code Legend.	12-8

About this Guide

This failover/failback procedures guide provides information to help you:

- Understand basic Data Replication Manager failover and failback concepts.
- Determine when a failover is the appropriate action.
- Determine which failover/failback procedure is the right action for your current situation.
- Perform the actual failover and failback procedures.
- Contact technical support for additional assistance.

What's New

This release of the *Compaq SANworks™ Data Replication Manager HSG80 ACS Version 8.6-4P Failover/Failback Procedures Guide* differs from the November 2001 release (part number AA-RPJ0B-TE) in the following ways:

- Novell 6.0 is now supported. The subjects of NetWare traditional and logical volumes have been added to the Novell-specific procedures in several chapters.

Intended Audience

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

- *Compaq StorageWorks™ ACS Version 8.6-4P* for their Data Replication Manager (DRM) storage system.
- Administration of the various operating systems used by the hosts in their heterogeneous SAN.

Related Documentation

The following table lists some of the documents that you may need to reference when connecting, configuring, and operating your DRM solution.

Document Title	Part Number
Compaq StorageWorks Fibre Channel Storage Switch Service Guide	AA-RHBZA-TE
Compaq StorageWorks Fibre Channel Storage Switch User's Guide	AA-RHBYA-TE
Compaq StorageWorks Fibre Channel SAN Switch Management Guide	AA-RMMJA-TE
Compaq StorageWorks 64-Bit/33-MHz Fibre Channel Host Bus Adapter Installation Guide	AA-RKPDB-TE
Compaq KGPSA-BC PCI-to-Optical Fibre Channel Host Bus Adapter User's Guide	AA-RF2JB-TE
Compaq StorageWorks Ultra SCSI RAID Enclosure (DS-BA370-Series) User's Guide	EK-BA370-UG
Compaq StorageWorks Command Console Version 2.2 (HSG80) for RA8000/ESA12000 User's Guide	AA-RFA2D-TE
Compaq StorageWorks Model 2100 and 2200 Ultra SCSI Controller Enclosure User Guide	EK-SE2C8-UA. B01
Compaq StorageWorks Enclosure 4200 Family LVD Disk Enclosure User Guide	EK-SW2ZS-UA. B01
Compaq StorageWorks SAN Switch Zoning Reference Guide	EK-P20ZG-GA. A01
Compaq StorageWorks Heterogeneous Open SAN Design Reference Guide	AA-RMPNA-TE
Compaq StorageWorks RA8000/ESA12000 and MA8000/EMA12000 Fibre Channel Solution Software Version 8.5b for Windows NT or Windows 2000 on X86 Platforms Installation Reference Guide	AA-RFA9E-TE
Compaq StorageWorks RA8000/ESA12000 and MA8000/EMA12000 Solution Software V8.5b for OpenVMS Installation Reference Guide	AA-RH4BC-TE

Document Title	Part Number
Compaq StorageWorks RA8000/ESA12000 and MA8000/EMA12000 Solution Software V8.5c for Novell NetWare Installation Reference Guide	AA-RFB9D-TE
Compaq SANworks Secure Path Version 3.0 for Novell Netware Installation and Reference Guide	AA-RN72A-TE
Compaq SANworks Data Replication Manager HSG80 ACS Version 8.6-4P Configuration User Guide	AA-RHPZC-TE
Compaq SANworks Data Replication Manager HSG80 ACS Version 8.6-1P Scripting User Guide	EK-DRMSD-OA
Compaq SANworks Data Replication Manager HSG80 ACS Version 8.6-4P Release Notes	AA-RPJ2C-TE
Compaq StorageWorks HSG80 Array Controller Version 8.6 Troubleshooting Reference Guide	EK-G80TR-SA
Compaq SANworks Secure Path Version 2.1A/2.1C for Sun Solaris Installation and Reference Guide	AA-RYKDB-TE
Compaq SANworks Secure Path Version 2.0 for IBM AIX Installation and Reference Guide	AA-RLTOA-TE
Compaq SANworks Secure Path Version 3.0 for Novell Netware Installation and Reference Guide	AA-RN72A-TE
Compaq SANworks Secure Path Version 3.1 for Microsoft Windows Installation and Reference Guide	AA-RL4SC-TE
Compaq StorageWorks HSG80 Array Controller ACS Version 8.5 Configuration Guide	EK-HSG85-CG
Compaq StorageWorks HSG80 Array Controller ACS V8.6 CLI Reference Guide	EK-G80CL-RA
Compaq StorageWorks HSG80 Array Controller ACS V8.6 Maintenance and Service Guide	EK-G80MS-SA

Software and Firmware Revision Levels

A list of the most current software, firmware, patches, drivers, and so on, for each of the supported operating systems in your DRM solution can be found at the following website:

<http://www.compaq.com/products/sanworks/drm/index.html>.

Follow the Software Support Matrices link, then choose your operating system.

Prerequisites

Compaq recommends that you rehearse or practice the procedures in this book so that you will be prepared to perform failover and failback quickly and accurately during a crisis.

Document Conventions

The conventions included in Table 1 apply in most cases.

Table 1: Document Conventions

Element	Convention
Key names, menu items, buttons, and dialog box titles	Bold
File names and application names	<i>Italics</i>
User input, command names, system responses (output and messages)	Monospace font COMMAND NAMES are uppercase unless they are case sensitive
Variables	<i>Monospace, italic font</i>
Website addresses	Sans serif font (http://www.compaq.com)

Symbols in Text

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



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



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

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

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

Symbols on Equipment



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

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



Any RJ-45 receptacle marked with these symbols indicates a network interface connection.

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



Any surface or area of the equipment marked with these symbols indicates the presence of a hot surface or hot component. Contact with this surface could result in injury.

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



Power supplies or systems marked with these symbols indicate the presence of multiple sources of power.

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



Any product or assembly marked with these symbols indicates that the component exceeds the recommended weight for one individual to handle safely.

WARNING: To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manually handling material.

Rack Stability



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

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

Getting Help

If you still have a question after reading this guide, contact service representatives or visit our website.

Compaq Technical Support

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

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

Outside North America, call Compaq technical support at the nearest location. Telephone numbers for worldwide technical support are listed on the Compaq website: <http://www.compaq.com>.

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)
- Product serial numbers

- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions.

Compaq Website

The Compaq website has the latest information on this product, as well as the latest drivers. Access the Compaq website at: <http://www.compaq.com/storage>. From this website, select the appropriate product or solution.

Compaq Authorized Reseller

For the name of your nearest Compaq Authorized Reseller:

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

Introduction to Failover/Failback

This chapter provides a general description of *SANworks*TM Data Replication Manager by Compaq and introduces the concepts of failover and failback. It also discusses process resumption options for special circumstances and provides a decision logic table to guide you in selecting the appropriate failover/failback or process continuation procedure for your current situation.

This chapter covers the following topics:

- “Data Replication Manager Overview” on page 1–2
 - “Peer-to-Peer Remote Copy Function” on page 1–2
 - “Hardware Redundancy” on page 1–2
- “Failover and Failback” on page 1–3
 - “Failover” on page 1–4
 - “Failback” on page 1–6
 - “Failsafe-Locked and Normal Modes” on page 1–6
- “Possible Event Scenarios” on page 1–7
- “Planned System Power Up or Power Down” on page 1–11
- “Using Scripts to Automate Failover and Failback Procedures” on page 1–12
 - “Overview” on page 1–12
 - “Requirements” on page 1–12
 - “How Scripts Work” on page 1–13

Data Replication Manager Overview

Data Replication Manager (DRM) provides a disaster-tolerant (DT) solution through the use of hardware redundancy and data replication across multiple sites. The sites can be near each other or separated by some distance.

A single DT DRM configuration requires two HSG80 Array Controller subsystems—one at the local or initiator site, and one at the remote or target site. For installations with multiple initiator subsystems, there can be an equal number of unique target sites, one per pair of initiator controllers.

A DRM configuration consists of paired sites. The *initiator* site carries out primary data processing. *Target* sites are used for data replication. Data processing occurs at the initiator site and the data is replicated or mirrored to the target sites. If a significant failure occurs at the initiator site, data processing can be resumed at the target sites, where the data is intact.

The DRM sites are connected over some distance by fiber optic cable or asynchronous transfer mode (ATM). DRM uses Fibre Channel switches to send the data between the sites. If the sites are too distant to communicate via Fibre Channel, other hardware may be used to connect the sites.

Peer-to-Peer Remote Copy Function

DRM uses the peer-to-peer remote copy function of the HSG80 controller to achieve data replication. HSG80 controller pairs at the initiator site are connected to their partner HSG80 controller pairs at the target site. Remote copy sets are created from units at the initiator and target sites. These remote copy sets contain storage devices that are mirrors of each other. As data is written to a unit at the initiator site, it is mirrored to its remote copy set partner unit at the target site.

Hardware Redundancy

DRM requires hardware redundancy. In the event of single component failure at a site, DRM fails over to a redundant component at that site to allow continued operations. For example, if one of the dual-redundant Fibre Channel links between the sites fails, DRM switches to the other link.

Failover and Failback

The HSG80 controllers provide *site failover* and *failback* capabilities in case of failures, for planned maintenance, or for site role reversal. Failover makes the data available at the target site after a failure. Failback moves data operations back to the initiator once it has been brought back on line.

Failover and failback require some level of operator intervention, and both require preparation at the initiator and target sites. In all situations, you must decide whether or not a failover is the best course of action. In situations where the failure is limited to failure of a single switch, a single cable, a single storage set, or the like, the least disruptive action may be to quickly repair the failed component instead of performing a site failover.

The example failover and failback procedures in this chapter use fictional “Building A” as the initiator site and “Building B” as the target site. The examples show the following procedures:

- Failover from Building A (initiator) to Building B (target)
- Failback from Building B (target) back to Building A (initiator).

Figure 1–1 illustrates a basic Data Replication Manager configuration.

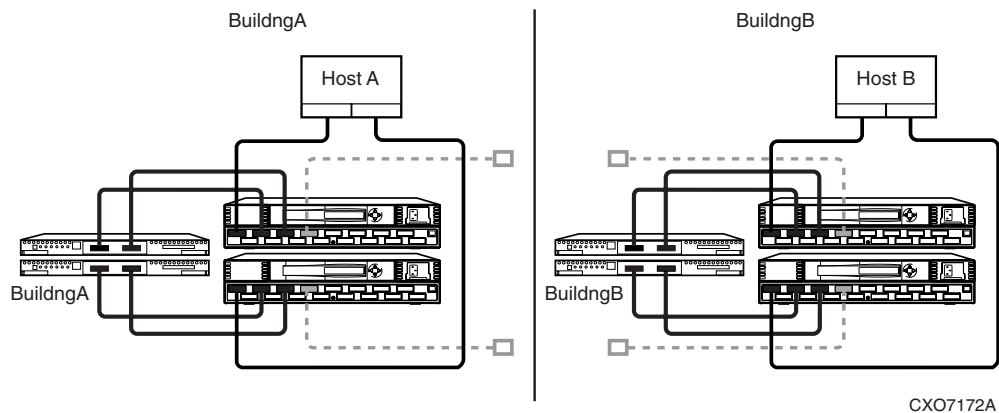


Figure 1–1: Basic Data Replication Manager configuration

NOTE: This document consistently refers to Building A as the initiator site and Building B as the target site. This does not change, even after failover has occurred to Building B (and before failback has occurred to Building A). While in failover mode, the controllers in Building B are acting as the *initiator* for all remote copy sets, but are still referred to as the *target* in this document.

Once the failback procedure is completed, the controllers in Building A resume their role as the initiator for remote copy sets.

IMPORTANT: Be careful that you don't start a site failover or site failback process too soon. You must wait a minimum of 15 minutes from the completion of a site failover process to begin a site failback procedure. You must also wait a minimum of 15 minutes from the completion of a site failback process to begin a site failover procedure.

Failover

Controller failover is the process that takes place when one controller in a dual-redundant configuration assumes the workload of a failed or redirected companion controller in the same cabinet. *Site failover* is the process that takes place when storage processing is moved from one pair of controllers to another. All processing is shifted to the target (remote) site. This is possible because all data generated at the initiator site has been replicated at the target site, in readiness for such a situation. This book is about site failover and not controller failover within a cabinet.

The site failover method is determined by the severity of the failure or the reason for the failover. A *planned failover* can be used for situations such as an anticipated power disruption, scheduled equipment maintenance at the local site, or the need to transfer operations to another site. An *unplanned failover* is used for events such as multiple controller failures, multiple host failures, or an unplanned power outage at the local site.

After failover has started, it continues until the failure at the initiator site is remedied, and the processing is returned to the initiator (local) site through the failback process.

If the initiator site fails, or if you are planning downtime at the initiator site, you must decide whether to perform a site failover to the target site.

When you perform a failover, the target site assumes the role of the initiator and accesses data until the problem is resolved and you perform a failback. By transferring control of system operation to the target site, you can ensure minimal interruption in data access after a failure.

NOTE: When you perform a site failover operation, you must failover *all* components. Therefore, if only one component has failed, fixing that single component may be preferable to performing a complete failover.

IMPORTANT: Always verify that all components at the target site are operational before you begin the site failover.

Table 1–1 outlines example situations that call for a failover and those that do not.

Table 1–1: When and When Not to Failover

Type of Failure	Recommended Action	
	Remote Copy Set Error_Mode = Normal	Remote Copy Set Error_Mode = Failsafe
Total initiator site loss	Manual intervention to fail over data and processing to target site	Manual intervention to fail over data and processing to target site
Loss of initiator site fabric	Manual intervention to fail over data and processing to target site	Manual intervention to fail over data and processing to target site
Loss of initiator controller pair	Manual intervention to fail over data to target site, and restart of processing at both sites	Manual intervention to fail over data to target site, and restart of processing at both sites
Loss of all intersite links	Failover not necessary	Decide on which site should continue processing: continue at initiator site or failover to target site
Total target site loss	Failover not necessary	Manually continue processing at initiator site
Loss of target fabric	Failover not necessary	Manually continue processing at initiator site
Loss of target controller pair	Failover not necessary	Manually continue processing at initiator and target sites
Loss of single initiator controller	Failover not necessary	Failover not necessary
Loss of both initiator switches	Manual intervention to fail over data to target site, and restart of processing at both sites	Manual intervention to fail over data to target site, and restart of processing at both sites
Loss of single initiator switch	Failover not necessary	Failover not necessary
Extended power outage at initiator site	Manual intervention to fail over data and processing to target site	Manual intervention to fail over data and processing to target site

Table 1–1: When and When Not to Failover (Continued)

Type of Failure	Recommended Action	
	Remote Copy Set Error_Mode = Normal	Remote Copy Set Error_Mode = Failsafe
Loss of both host bus adapters (non-clustered hosts)	Manual intervention to fail over data to target site, and restart of processing at both sites	Manual intervention to fail over data to target site, and restart of processing at both sites
Loss of single disk in redundant storage	Failover not necessary	Failover not necessary
Loss of single storage set	Failover not necessary	Failover not necessary
Loss of single host of cluster	Failover not necessary	Failover not necessary

NOTE: If one host in a multi-host environment fails, you must decide whether or not a failover is the best course of action.

Failback

Controller failback takes place when one controller in a dual-redundant configuration has been repaired and assumes the workload that it had prior to the failure. *Site failback* is the process that takes place when storage processing is moved back to the original initiator site after whatever failed at the initiator site is repaired or replaced. The failback method (*full copy* or *fast failback*) is determined by the enabling of the write history logging or failsafe switches, the selected mode of operation (synchronous or asynchronous), and whether the failover is planned or unplanned. This book is about site failback and not controller failback within a cabinet.

Failsafe-Locked and Normal Modes

Failsafe-locked is an error mode that you can set to cease initiator site I/O in the event that the target becomes inaccessible. Several of the procedures in this document provide instructions on how to transition between failsafe-locked mode and normal mode, so that you can resume processing at the initiator site. Transitioning between failsafe and normal modes does not constitute an actual failover and failback event.

Possible Event Scenarios

If failover becomes necessary, one of the following scenarios will in all likelihood describe your current situation or your desired action.

Compaq recommends that you rehearse or practice the procedures in this book so that you will be prepared to perform failover and failback quickly and accurately during a crisis.

Unplanned Site Failover with Full Failback

Situation: You have experienced an unplanned loss of the initiator site. The loss could have been caused by a power failure or other event that did not damage initiator site hardware. The duration of the outage at the initiator is unknown. The DRM hardware components (hosts, controllers, switches, for example) at the initiator site will remain intact.

Action: You will perform a failover to the target site. When the power is returned to the initiator site and it is back online, you will perform a full failback to the initiator site. Follow the procedure in Chapter 2.

Unplanned Loss of Target While in Failsafe Mode

Situation: You have experienced an unplanned loss of target site function due to failure of the intersite links or similar event such as loss of power at the target, loss of both target switches, and so on. The duration of the outage is unknown. The remote copy sets are in failsafe mode and host I/O is paused.

Action: You will remove the targets, then resume host I/O until the connection to the target site is re-established. Follow the procedure in Chapter 3.

Unplanned Loss of Target While in Normal Mode

Situation: Similar to the previous scenario in that you have experienced an unplanned loss of target site function due to failure of the intersite links. However, the remote copy sets are in normal mode. The duration of the outage is unknown, but longer than can be accommodated with write history logging.

Action: You will allow host access to the remote copy sets, then resume operations. Follow the procedure in Chapter 4.

Short Duration Initiator Site Maintenance

Situation: You will be performing planned maintenance at the initiator site. The maintenance will be completed within a relatively short period of time (within several hours).

Action: You will perform a failover to the target site. Because of the short duration of the planned outage, the write history log will be able to accommodate the accumulated writes. When the initiator is operational and back online, you will perform a fast failback to the initiator with the merge function. Follow the procedure in Chapter 5.

Resumption of Replication After Short Planned Loss of Target

Situation: You will be bringing the target site down for planned maintenance. The remote copy sets are in failsafe mode. The duration of the outage at the target site is relatively short (up to several hours).

Action: You will not be performing failover or failback, but you will resume replication after the target site is operational and back online. Follow the procedure in Chapter 6.

Extended Duration Initiator Site Maintenance

Situation: You will be performing planned maintenance at the initiator site. The maintenance will not be completed within a relatively short period of time.

Action: You will perform a failover to the target site. Because of the longer duration of the planned outage, the write history log will not be able to accommodate the accumulated writes. Because the write history log cannot capture all host I/O, you will perform a full failback to the initiator when the initiator is operational and back online. Follow the procedure in Chapter 7.

Resumption of Replication After Extended Planned Loss of Target

Situation: The target site will be shut down for an extended length of time, perhaps for maintenance or for a planned power outage. The remote copy set's error mode is set for failsafe.

Action: You will reset the remote copy set's error mode to normal to allow host I/O to continue while the target site is offline. Because there is no log unit configured, you will perform a full copy when the target site is back online. Follow the procedure in Chapter 8.

Unplanned Site Failover Due to Disaster at Initiator

Situation: A disaster of some type of disaster (lightning, flood, fire, severe equipment failure, or the like) has damaged the initiator site.

Action: You will perform an unplanned site failover to the target site. When the damaged components at the initiator site (hosts, controllers, and switches, for example) have been repaired, and the site is operational and back online, you will perform a failback to the new hardware. Follow the procedure in Chapter 9.

Planned Role Reversal

Situation: You will be performing a planned move of initiator operations from the initiator site to an alternate (target) site.

Action: You will prepare the initiator site for the failover, then perform a failover to the alternate site. The original initiator site remains intact, operational, and online as the target during the role reversal. You will then perform a role reversal failback to the original initiator site, when desired. Follow the procedure in Chapter 10.

Recovery from Disaster During Planned Role Reversal

Situation: You have performed a planned role reversal, as in the above scenario. However, during the time that the initiator/target roles are reversed, access to the target site (the original initiator site) has been lost.

Action: When access to the initiator site has been reestablished, you will recreate the remote copy sets so that the data is copied from the acting initiator (old target site) to the acting target (old initiator site) prior to performing a failback operation. Follow the procedure in Chapter 11.

Summary of Procedure Choices

Table 1–2 summarizes the information in the preceding scenarios and directs you to the appropriate chapter in this document for the procedures that you should follow. The table also indicates whether the procedure is available as a scripted procedure.

Table 1–2: Procedure Choices

Event or Condition	Anticipated Duration of Event	Initiator Mode of Operation	Procedure to Follow	Scripting Available
Unplanned loss of initiator site function. Initiator site hardware will not be replaced.	Unknown	Normal or failsafe	Chapter 2: Unplanned Site Failover with Full Failback	Yes
Unplanned loss of target site function. Remote copy sets are in failsafe mode and targets are removed.	Unknown	Failsafe	Chapter 3: Resumption of Operations After Unplanned Loss of Target Site: Failsafe Mode	Yes
Unplanned loss of target site function. Remote copy sets are in normal mode and targets are removed.	Unknown	Normal	Chapter 4: Resumption of Operations After Unplanned Loss of Target Site: Normal Mode	Yes
Planned maintenance outage at initiator site.	Short—up to several hours	Normal or failsafe	Chapter 5: Short Planned Site Failover With Fast Failback	Yes
Planned maintenance outage at target site.	Short—up to several hours	Failsafe	Chapter 6: Resumption of Replication After Short Planned Loss of Target	No
Planned maintenance outage at initiator site.	Extended—many hours or longer	Normal or failsafe	Chapter 7: Extended Planned Site Failover With Full Failback	Yes
Planned maintenance at target site.	Extended—many hours or longer	Failsafe	Chapter 8: Resumption of Replication After Extended Planned Loss of Target	Yes

Table 1–2: Procedure Choices (Continued)

Event or Condition	Anticipated Duration of Event	Initiator Mode of Operation	Procedure to Follow	Scripting Available
Unplanned loss of initiator site function. Initiator site hardware will be new.	Unknown	Normal or failsafe	Chapter 9: Unplanned Site Failover With Failback To New Hardware	Yes
Planned change of operations from initiator site to alternate site (role reversal). Initiator site remains operational after role reversal.	Unknown	Normal or failsafe	Chapter 10: Planned Site Role Reversal	Yes
Planned change of operations from initiator site to alternate site (role reversal). Initiator site remains operational. Disaster occurs at initiator site after role reversal.	Unknown	Normal or failsafe	Chapter 11: Disaster Recovery After Role Reversal	No

Planned System Power Up or Power Down

If you need to power up or power down your DRM system, follow the procedure in Appendix B.

Using Scripts to Automate Failover and Failback Procedures

Scripts provide an automated alternative to a manual command entry process for failover and failback operations. The following sections give information about the scripting process.

Overview

You can perform failover and failback procedures manually, by issuing a complex series of Command Line Interpreter (CLI) commands. But by using *scripts*, you can automate the process and greatly reduce the need for CLI commands. After you have set up your scripting configuration, you run those scripts, which issue the appropriate CLI commands. However, you must still be able to perform a failover or failback manually with CLI commands if the scripts encounter an abnormal condition that keeps them from running properly.

Using scripts in a DRM environment makes it easier to perform failover and failback. By using one launch file, you can start a complete failover or failback sequence. This shortens downtime by eliminating the delay between command entries. Using scripts also ensures that the sequence of commands has been predetermined in a calm environment, rather than during a crisis, when mistakes are more common. The result is a failover and failback process that is timely, consistent, and efficient.

Requirements

Scripting requires the following components:

- The Compaq DRM Scripting Kit
- A Perl interpreter
- Compaq *SANworks* Command Scripter
- *SANworks Data Replication Manager by Compaq HSG80 ACS Version 8.6-1P Scripting User Guide*

How Scripts Work

Failover and failback scripts are written in the Perl programming language and reside on the host's local hard drive. For redundancy, the scripts should reside on a host on both the initiator and target sites.

The failover and failback scripts use two user-customized file types to provide variable information: a *configuration file* and an *application action list*.

The configuration files and the application action list are system specific. You must tailor the configuration files and action list for your specific configuration, and for your failover and failback preferences. Your scripts can then use these files to perform failover and failback.

To perform automated failover or failback, you invoke a failover or failback script by running a *launch file* from a command prompt on the system console. Then:

1. The Perl interpreter processes the script, based on the information in the configuration file and the application action list.
2. The script reads the *control table*, which controls the order of CLI commands to be issued, and sends the appropriate sequence of CLI commands (for the controller configuration specified in the configuration file) to the Command Scriptor.
3. The Command Scriptor sends the commands to the HSG80 controller over the Fibre Channel bus and relays SHOW command verification back for the scripts.

IMPORTANT: If you will be using scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention (remote copy sets, stripesets, mirrorsets, RAIDsets, association sets, and connections)—use underscores instead. Dashes are not allowed by the Perl scripting language.

Refer to the *SANworks Data Replication Manager by Compaq HSG80 ACS Version 8.6-1P Scripting User Guide* for more information on the scripting process.

Unplanned Site Failover with Full Failback Procedure

In this situation you have experienced an unplanned loss of the initiator site. The loss could have been caused by a power failure or other event that did not damage initiator site hardware. The duration of the outage at the initiator is unknown. The DRM hardware components (hosts, controllers, switches, for example) at the initiator site will remain intact. You will perform a failover to the target site. When the power is returned to the initiator site and it is back online, you will perform a full failback to the initiator site.

This chapter contains the following procedures to ensure that unplanned failover and subsequent full failback function properly:

- “Unplanned Failover” on page 2–2
 - “Target Site Failover Procedure” on page 2–2
- “Full Failback” on page 2–12
 - “Initiator Site Preparation Procedure” on page 2–12
 - “Target Site Copy Data Procedure” on page 2–17
 - “Initiator Site Return Control Procedure” on page 2–21
 - “Target Site Restore Procedure” on page 2–22
 - “Initiator Site Restoration of Target Connections Procedure” on page 2–24

NOTE: In this chapter, *initiator* site procedure steps are identified by an arrow symbol ► in the margin. *Target* site procedure steps are identified by a target symbol 🎯 in the margin.

NOTE: Some example displays illustrate confirmation messages with the event log symbol (%EVL) and an instance code. Compare the instance code in the example with the instance code you receive. If the numbers are the same, you have performed the previous command correctly and have achieved the desired results. Note that you will be able to see these screens only if you are working from the controller to which the LUNs are online. Refer to the Troubleshooting chapter for more information on instance codes and their meanings.

Example displays may also contain bold text to identify information that is the most pertinent in the example. In many cases, items shown in bold text will help you verify the results of a previous command.

Unplanned Failover

Use the Unplanned Failover in conjunction with a Full Failback whenever the initiator site cannot carry out its function.

Target Site Failover Procedure

1. Make sure that the connection between sites is not restored, by entering the following CLI commands:

```
SET THIS CONTROLLER PORT_2_TOPOLOGY = OFFLINE
SET OTHER CONTROLLER PORT_2_TOPOLOGY = OFFLINE
```

2. Verify that the connection is offline by entering the following CLI commands:

```
SHOW_THIS_CONTROLLER
SHOW_OTHER_CONTROLLER
```

You will see a display similar to that in Example Display 1.

Example Display 1

```
BuildngBTop> show this_controller
Controller:
  HSG80 ZG94115654 Software V86-1P, Hardware E10
  NODE_ID           = 5000-1FE1-0000-4250
  ALLOCATION_CLASS   = 0
  SCSI_VERSION      = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG94319198
  In dual-redundant configuration
  Device Port SCSI address 7
  Time: 10-MAY-2001 16:42:49
  Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-4253
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address          = 260213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-4254
  PORT_2_TOPOLOGY = OFFLINE (offline)
  REMOTE_COPY     = BUILDNGB
.
.
.
BuildngBTop> show other_controller
Controller:
  HSG80 ZG94319198 Software V86-1P, Hardware E10
  NODE_ID           = 5000-1FE1-0000-4250
  ALLOCATION_CLASS   = 0
  SCSI_VERSION      = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG94115654
  In dual-redundant configuration
  Device Port SCSI address 6
```



```

Time: 10-MAY-2001 16:43:12
Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-4251
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address          = 200213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-4252
  PORT_2_TOPOLOGY = OFFLINE (offline)
  REMOTE_COPY     = BUILDNGB
.
.
.

```

- 3. At the target site, the remote copy set units must be preferred to one controller or the other.
 - a. Use the following CLI command to check for the preferred path:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 2.

Example Display 2

```

BuildngBTop> show units full
LUN
-----
D1
LUN ID:          6000-1FE1-0000-4250-0009-9411-5654-003E
NOIDENTIFIER
Switches:
  RUN              NOWRITE_PROTECT          READ_CACHE
  READAHEAD_CACHE WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 128
  MAX_WRITE_CACHED_TRANSFER_SIZE = 128
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD
State:
  ONLINE to the other controller
  PREFERRED_PATH = THIS_CONTROLLER
  Target NORMAL
Size:          17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
D2
LUN ID:          6000-1FE1-0000-4250-0009-9411-5654-003F
NOIDENTIFIER
Switches:
  RUN              NOWRITE_PROTECT          READ_CACHE
  READAHEAD_CACHE WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = OTHER_CONTROLLER
  Target NORMAL

```

```
Size: 17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
```

- b. If the remote copy set units are not currently preferred, use the following CLI command:

```
SET UnitName PREFERRED_PATH = THIS_CONTROLLER
Example: set d1 preferred_path = this_controller
or
SET UnitName PREFERRED_PATH = OTHER_CONTROLLER
Example: set d2 preferred_path = other_controller
```

Repeat this step for each remote copy set unit.

4. Use the following CLI command to failover each remote copy set (maximum of 12 per subsystem):

```
SITE_FAILOVER InitiatorRemoteCopyName\RemoteCopySetName
Example: site_failover buildngA\rcl
```

You will see a confirmation message, as shown in Example Display 3.

Example Display 3

```
BuildngBTop> site_failover buildngA\rcl
%EVL--BuildngBTop> --10-MAY-2001 16:48:08-- Instance Code: 0E010064
Template: 144.(90)
.
.
Instance Code: 0E010064
```

Repeat this step for all remote copy sets.

5. Remove the targets with the following CLI command:

```
SET RemoteCopySetName REMOVE = InitiatorRemoteCopyName\UnitNumber
Example: set rcl remove = buildngA\d1
```

You will see a confirmation message, as shown in Example Display 4.

Example Display 4

```
BuildngBTop> set rcs1 remove = buildngA\d1
%EVL--BuildngBTop> --10-MAY-2001 16:49:55-- Instance Code: 0E078A01
Template: 144.(90)
.
.
Instance Code: 0E078A01
```

6. Verify that you have removed the targets by entering the following CLI command:

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to that in Example Display 5.

Example Display 5

```
BuildngBTop> show remote_copy_sets full
Name                               Uses                               Used by
-----
RCS1      remote copy                       D1
Reported LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0134
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGB\D1) state:
  ONLINE to the other controller
No targets
```

Repeat this step for all remote copy sets.

7. Obtain your record of SHOW command output that details the original initiator configuration. Using the output as a reference, create association sets to duplicate those that were on the initiator. For information on how to create association sets, see Appendix C.

Repeat this step for each association set. You can set up write history logging after targets are added back to the configuration later in this chapter.

IMPORTANT: If you will be using scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention (remote copy sets, stripesets, mirrorsets, RAIDsets, association sets, and connections)—use underscores instead. Dashes are not allowed by the Perl scripting language.

- 8. Enable host access to all remote copy set units at the target site with the following CLI command:

```
SET UnitName ENABLE = TargetHostConnectionNamex,  
TargetHostConnectionNamey
```

Example: set d1 enable = hostb1,hostb2

You will see a display similar to that in Example Display 6.

Example Display 6

```
BuildngBTop> set d1 enable=hostb1,hostb2  
Warning 1000: Other host(s) in addition to the one(s) specified can still  
access this unit. If you wish to enable ONLY the host(s)  
specified, disable all access paths (DISABLE_ACCESS=ALL), then  
again enable the ones specified
```

Repeat this step for each remote copy set unit.

- 9. If you do not recall a target host connection name, use the following command:

```
SHOW CONNECTIONS
```

You will see a display similar to that in Example Display 7.

Example Display 7

```
BuildngBTop> show connections
```

Connection Name	Operating system	Controller	Port	Address	Status	Unit Offset
BUILDNGAA	PPRC_TARGET HOST_ID=5000-1FE1-0000-01F0	THIS	2		offline	0
				ADAPTER_ID=5000-1FE1-0000-01F4		
BUILDNGAB	PPRC_TARGET HOST_ID=5000-1FE1-0000-01F0	OTHER	2		offline	0
				ADAPTER_ID=5000-1FE1-0000-01F2		
BUILDNGAC	PPRC_INITIATOR HOST_ID=5000-1FE1-0000-01F0	THIS	2	220413	OL this	0
				ADAPTER_ID=5000-1FE1-0000-01F4		
BUILDNGAD	PPRC_INITIATOR HOST_ID=5000-1FE1-0000-01F0	OTHER	2	250413	OL other	0
				ADAPTER_ID=5000-1FE1-0000-01F2		
HOSTA1	WINNT HOST_ID=1000-0000-C920-A7B9	THIS	1	260013	OL this	0
				ADAPTER_ID=1000-0000-C920-A7B9		
HOSTA2	WINNT HOST_ID=1000-0000-C921-3F4E	OTHER	1	200013	OL other	0
				ADAPTER_ID=1000-0000-C921-3F4E		
HOSTB1	WINNT HOST_ID=1000-0000-C921-3E98	THIS	1	220013	OL this	0
				ADAPTER_ID=1000-0000-C921-3E98		
HOSTB2	WINNT HOST_ID=1000-0000-C921-3EFC	OTHER	1	250013	OL other	0
				ADAPTER_ID=1000-0000-C921-3EFC		

- ⑩ 10. Verify the target site hosts access with the following CLI command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 8.

Example Display 8

```
BuildngBTop> show units full
-----
LUN                               Uses                               Used by
-----
D1                                  DISK10000                          BUILDNGB\RCS1
LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003E
NOIDENTIFIER
Switches:
  RUN                               NOWRITE_PROTECT                     READ_CACHE
  READAHEAD_CACHE                   WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD, HOSTB1, HOSTB2
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = THIS_CONTROLLER
Size: 17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )

D2                                  DISK20000                          BUILDNGB\RCS2
LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003F
NOIDENTIFIER
Switches:
  RUN                               NOWRITE_PROTECT                     READ_CACHE
  READAHEAD_CACHE                   WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD, HOSTB1, HOSTB2
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = OTHER_CONTROLLER
Size: 17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
```

In the Access field of the display, all units that are used by remote copy sets will show that both the target host and the initiator controller connections are enabled.

- ⑪ 11. If desired, you can enhance host I/O performance by resetting the maximum cached transfer size to the original value used on the initiator. Use this command:

```
SET UnitName MAXIMUM_CACHED_TRANSFER_SIZE = InitiatorValue
```

```
Example: set d1 maximum_cached_transfer_size = 32
```

Repeat this step for all remote copy set units.

NOTE: The default initiator value for maximum cached transfer size is 32.

- ② 12. Verify that the maximum cached transfer size was correctly modified with the following command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 9.

Example Display 9

```
BuildngBTop> show units full
-----
LUN                               Uses                               Used by
-----
D1                                  DISK10000                          BUILDNGB\RCS1
LUN ID:        6000-1FE1-0000-4250-0009-9411-5654-003E
NOIDENTIFIER
Switches:
  RUN          NOWRITE_PROTECT      READ_CACHE
  READAHEAD_CACHE  WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD,  HOSTB1,  HOSTB2
State:
  ONLINE to the other controller
  PREFERRED_PATH = THIS_CONTROLLER
Size:        17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
D2                                  DISK20000                          BUILDNGA\RCS2
LUN ID:        6000-1FE1-0000-4250-0009-9411-5654-003F
NOIDENTIFIER
Switches:
  RUN          NOWRITE_PROTECT      READ_CACHE
  READAHEAD_CACHE  WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
.
.
.
```

- ② 13. Allow hosts to recognize new units. Follow the steps listed below for each operating system in your heterogeneous configuration:
 - a. **Compaq OpenVMS™**: If the target site hosts are shut down, boot them now. Booting the hosts enables OpenVMS to recognize the drives.

If the target site hosts are not shut down, use the following command from a privileged account to enable OpenVMS to recognize the drives:

```
MCR SYSMAN IO AUTOCONFIGURE/LOG
```

Mount the volumes associated with the remote copy set LUNs on each host with access to those LUNs.

- b. **Compaq Tru64™ UNIX:** If the target site hosts are shut down, boot them now. Booting the hosts enables Tru64 UNIX to recognize the drives.

If the target site hosts are not shut down, use the following command to recognize the drives:

```
hwmgr - scan scsi
```

This might take a while for large configurations. If this is the case, scan only those SCSI buses that have new units added. Scan only one bus at a time. Use the following command:

```
hwmgr -scan scsi -bus x
```

where x is the SCSI bus number.

- c. **HP-UX:**

- 1) If the target site hosts are shut down, boot them now. Booting the hosts enables HP-UX to recognize the drives.

If the target site hosts are not shut down, use the following command to enable HP-UX to recognize the drives and verify that they are present. This command will display only the previously configured failed-over LUNs:

```
ioscan -fnCdisk
```

- 2) Continue with the following commands to access file systems on new failed-over LUNs. If you have no new failed-over LUNs, skip these substeps and go directly to the next step to mount the LUNs:

```
a. /opt/CPQswsp/spmgr display -u
```

```
b. /opt/CPQswsp/spmgr add WWN
```

Repeat this command for each un-attached WWN that was displayed.

```
c. ioscan -fnCdisk
```

If the device special files were not displayed, run `insf -e`, then run `ioscan -fnCdisk` again.

```
d. vgimport VolumeGroupName DeviceSpecialFile
```

Repeat this command for each new failed-over LUN.

- 3) Use the following command to mount the LUNs:

```
mount -a
```

NOTE: *VolumeGroupName* is the name of the volume group you originally created at the initiator site. The *DeviceSpecialFiles* are from the *ioscan* in the form of */dev/dsk/c_t_d_*.

For consistency, configure the same *DeviceSpecialFiles* with the same volume groups, logical volumes, and file systems for the failed-over LUNs at the target site with the same LUNs at the initiator site.

- d. **IBM AIX:** If the target site hosts are shut down, boot them now. Booting the hosts enables IBM AIX to recognize the drives.

If the target site hosts are not shut down, use the following commands to enable AIX to recognize the drives and verify that they are present:

```
cfgmgr -v  
lsdev -C disk
```

Use the following commands to access file systems on the failed-over LUNs:

```
importvg -y volumeGroupName hdiskx  
mount all
```

NOTE: *volumeGroupName* is the name of the volume group you originally created at the initiator site, and *x* is the number of the hdisk assigned to the failed-over LUN. If the *-y volumeGroupName* parameter is omitted, AIX will create a default volume group name for you, for example, *vg00*.

- e. **Microsoft Windows NT-X86:** Turn on or reboot the hosts at the target site and log in using an account that has administrative privileges. You should be able to see all of the units by choosing **My Computer**.
- f. **Microsoft Windows 2000:**

- 1) If you *have not* changed the *UNIT_OFFSET* of any host connections since the hosts have been booted, you do not need to reboot the initiator site hosts.

- a) On each host, log in using an account that has administrative privileges.

- b) Open **Computer Management** and click **Disk Management**.

- c) After **Disk Management** has initialized, go to the **Action** menu and click **Rescan Disks**. All of the failed over units should appear in the right-hand pane. If Secure Path is not installed correctly, you will see each unit twice.

2) If you *have* changed the UNIT_OFFSET of any host connections, you must reboot that host. After the server has rebooted, log in using an account that has administrative privileges. You will see all of the units in **Computer Management > Disk Management**. If Secure Path is not installed correctly, you will see each drive twice.

- g. **Novell NetWare:** If the target site hosts are shut down, boot them now. If you are using traditional NetWare volumes, booting the hosts allows Novell NetWare to recognize the drives and automatically mount the volumes. If you are using NSS logical volumes, booting the hosts will recognize the NSS pools and activate them. However, you must manually mount each individual NSS volume by typing `MOUNT VolumeName` at the NetWare console.

If the target site hosts are already up and running, or if they do not recognize the drives, issue the following command from the console before mounting the volumes:

```
SCAN FOR NEW DEVICES
```

Alternatively, you can use the `NWCONFIG` utility to issue this same command.

Next, mount the volumes with these commands:

```
MOUNT ALL (for traditional NetWare volumes)
```

```
MOUNT VolumeName (for NSS logical volumes).
```

- h. **SUN Solaris:** Turn on or reboot the hosts using the command `reboot -- -r` at the target site and log in using an account that has administrative privileges. You should be able to see all of the units by using the `format` command.

If Secure Path was not configured for these units, you will not see the drives. You will need to edit the WWLIDs in the file `/kernel/drv/ldLite.conf`. To find the new WWLIDs of the units, use the `SHOW Unitname` command on the controller. You may also need to adjust the files `/kernel/drv/mda.conf` and `/kernel/drv/sd.conf` to accommodate the extras LUNs. When you have edited `ldLite.conf`, `mda.conf`, and `sd.conf`, reboot the host using the `reboot -- -r` command. You should now be able to see the drives using the `format` command. Refer to the *Compaq SANworks Secure Path for Sun Solaris Installation and Reference Guide* for additional assistance.

This completes the failover procedure. When the problem that disabled the initiator site is remedied, proceed with the following Full Failback procedure.

Full Failback

Before performing a full failback, verify that your initiator controller configuration is the same as your target controller configuration.

Compare the status of the controllers, association sets, remote copy sets, units, and connections at the target site with those at the initiator site. A full procedure is detailed in Appendix A. Make sure that any status change is reflected on the target.

Full failback consists of the following procedures:

- Initiator Site Preparation Procedure
- Target Site Copy Data Procedure
- Initiator Site Return Control Procedure
- Target Site Restore Procedure
- Initiator Site Restoration of Target Connections Procedure

Initiator Site Preparation Procedure

- ▶ 1. Power up the controllers, if necessary. The procedure for power up is contained in Appendix B.
- ▶ 2. If the controllers were not powered down correctly, lost data may have been generated. Check all units for lost data with the following CLI command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 10.

Example Display 10

```
BuildngATop> show units full
-----
LUN                               Uses                               Used by
-----
D1                                DISK10000                          Buildnga\RCS1
LUN ID:                           6000-1FE1-0007-9DD0-0009-0510-3907-000C
NOIDENTIFIER
Switches:
  RUN                               NOWRITE_PROTECT                     READ_CACHE
  READAHEAD_CACHE                   WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 128
  MAX_WRITE_CACHED_TRANSFER_SIZE = 128
Access:
  BUILDNGBA, BUILDNGBB, BUILDNGBC, BUILDNGBD
State:
INOPERATIVE
Unit has lost data
UNKNOWN - Unit is no longer an initiator
```

```
PREFERRED_PATH = THIS_CONTROLLER
WRITE_PROTECT = DATA SAFETY
Size: NOT YET KNOWN
Geometry (C/H/S): NOT YET KNOWN
```

- a. If there is lost data, clear it for each applicable unit with the following CLI command:

```
CLEAR_ERRORS UnitName LOST_DATA
```

Example: `clear_errors d1 lost_data`

Repeat for all units with lost data.

- b. Verify that there is no lost data with the following CLI command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 11. If the lost data has been cleared, the display will indicate that the unit is **ONLINE**.

Example Display 11

```
BuildngATop> show units full
LUN                               Uses                               Used by
-----
D1                                DISK10000                          BUILDNGA\RCS1
LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0135
NOIDENTIFIER
Switches:
  RUN                               NOWRITE_PROTECT                     READ_CACHE
  READAHEAD_CACHE                   WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  BUILDNGBA, BUILDNGBB, BUILDNGBC, BUILDNGBD
State:
ONLINE to the other controller
  PREFERRED_PATH = OTHER_CONTROLLER
Size: 17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
```

- ▶ 3. Follow the steps listed below for each operating system in your heterogeneous configuration:
 - a. **Compaq OpenVMS:** If the operating system is up and running, and is being used exclusively for DRM operations, shut down the operating system and power off the hosts. If the operating system is being used for other applications, remove all I/O to the remote copy set LUNs that will be failed over, then dismount the volumes associated with these LUNs.

- b. **Compaq Tru64 UNIX:** If the operating system is up and running and is being used exclusively for DRM operations, shut down the operating system and power off the hosts. If the operating system is being used for other applications, remove all I/O and unmount all file system LUNs that have remote copy sets that will be failed over.
- c. **HP-UX:** If the operating system is up and running, remove all I/O to the remote copy set LUNs that will be failed over, then unmount the file systems associated with these LUNs.
- d. **IBM AIX:** If the operating system is up and running, remove all I/O to the remote copy set LUNs that will be failed over, then unmount the file systems associated with these LUNs.
- e. **Microsoft Windows NT-X86:** If the operating system is up and running, shut it down and power off the hosts.
- f. **Microsoft Windows 2000:** If the operating system is up and running, shut it down and power off the hosts.
- g. **Novell NetWare:** If the operating system is up and running, remove all I/O to the remote copy set LUNs that will be failed over, then dismount the volumes associated with these LUNs.

If you are using NetWare Cluster Services (NWCS), you must enter the `cluster down` command. You must also enter the `uldncs` (unload NetWare Cluster Services) command for all cluster nodes.



CAUTION: Failure to enter these two commands will cause all cluster nodes to abend.

- h. **SUN Solaris:** If the operating system is up and running and is being used exclusively for DRM operations, shut down the operating system and power off the hosts. If the operating system is being used for other applications, remove all I/O and unmount all volumes that have remote copy sets that will be failed over.
- ▶ 4. Disable host access to all remote copy set units by issuing the following CLI command:

```
SET UnitName DISABLE = InitiatorHostConnectionNamex,  
InitiatorHostConnectionNamey
```

Example: `set dl disable = hosta1,hosta2`

- ▶ 5. If you do not recall the initiator host name, use the following CLI command:

```
SHOW CONNECTIONS
```

- ▶ 6. Verify the lack of host access by entering the following CLI command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 12. Note that connections to HostA1 and HostA2 are missing from the Access field.

Example Display 12

```
BuildngATop> show units full
-----
LUN                                     Uses                                Used by
-----
D1                                     DISK10000                           BUILDNGA\RCS1
LUN ID:                               6000-1FE1-0000-01F0-0009-8490-6303-0134
NOIDENTIFIER
Switches:
  RUN                                  NOWRITE_PROTECT                       READ_CACHE
  READAHEAD_CACHE                     WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  BUILDNGBA, BUILDNGBB, BUILDNGBC, BUILDNGBD
State:
  ONLINE to the other controller
  PREFERRED_PATH = THIS_CONTROLLER
Size:                                  17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )

D2                                     DISK20000                           BUILDNGA\RCS2
LUN ID:                               6000-1FE1-0000-01F0-0009-8490-6303-0135
NOIDENTIFIER
Switches:
  RUN                                  NOWRITE_PROTECT                       READ_CACHE
  READAHEAD_CACHE                     WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  BUILDNGBA, BUILDNGBB, BUILDNGBC, BUILDNGBD
State:
  ONLINE to the other controller
  PREFERRED_PATH = OTHER_CONTROLLER
Size:                                  17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
```

- ▶ 7. Set maximum cached transfer size to 128 with the following CLI command:

```
SET unitname MAXIMUM_CACHED_TRANSFER_SIZE = 128
```

```
Example: set d1 maximum_cached_transfer_size = 128
```

Repeat this step for all remote copy set units.

NOTE: This command sets both the read and write maximum cached transfer size.

- ▶ 8. If write history logging is enabled, turn it off with the following CLI command:

```
SET AssociationSetName NOLOG_UNIT
```

Example: set as_d1 nolog_unit

Repeat for each association set.

- ▶ 9. If there are any association sets, delete them with the following CLI command:

```
DELETE AssociationSetName
```

Example: delete as_d1

Repeat for each association set.

- ▶ 10. Delete all remote copy sets using the following CLI command:

```
DELETE RemoteCopySetName
```

Example: delete rcs1

You will see a confirmation message, as shown in Example Display 13.

Example Display 13

```
BuildngATop> delete rcs1
```

```
%EVL--BuildngATop> --10-MAY-2001 17:31:51-- Instance Code: 0E020064  
Template: 144.(90)
```

```
.  
.  
.
```

```
Instance Code: 0E020064
```

Repeat this procedure for each remote copy set.

- ▶ 11. Continue with Full Failback at the target site with the Target Site Copy Data Procedure.

Target Site Copy Data Procedure

This section describes how to copy the data from the target site to the initiator site.

- ① 1. To restore the connections to the target site, issue the following CLI commands:

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

- ① 2. Verify that the connections are restored with the following CLI commands:

```
SHOW THIS_CONTROLLER
SHOW OTHER_CONTROLLER
```

You will see a display similar to that in Example Display 14.

Example Display 14

```
BuildngBTop> show this_controller
Controller:
    HSG80 ZG94115654 Software V86-1P, Hardware E10
    NODE_ID = 5000-1FE1-0000-4250
    ALLOCATION_CLASS = 0
    SCSI_VERSION = SCSI-3
    Configured for MULTIBUS_FAILOVER with ZG94319198
    In dual-redundant configuration
    Device Port SCSI address 7
    Time: 10-MAY-2001 17:34:11
    Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
    Reported PORT_ID = 5000-1FE1-0000-4253
    PORT_1_TOPOLOGY = FABRIC (fabric up)
    Address = 260213
Host PORT_2:
    Reported PORT_ID = 5000-1FE1-0000-4254
    PORT_2_TOPOLOGY = FABRIC (fabric up)
    Address = 260413
    REMOTE_COPY = BUILDNGB
.
.
.
BuildngBTop> show other_controller
Controller:
    HSG80 ZG94319198 Software V86-1P, Hardware E10
    NODE_ID = 5000-1FE1-0000-4250
    ALLOCATION_CLASS = 0
    SCSI_VERSION = SCSI-3
    Configured for MULTIBUS_FAILOVER with ZG94115654
    In dual-redundant configuration
    Device Port SCSI address 6
    Time: 10-MAY-2001 17:34:20
    Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
    Reported PORT_ID = 5000-1FE1-0000-4251
    PORT_1_TOPOLOGY = FABRIC (fabric up)
    Address = 200213
Host PORT_2:
    Reported PORT_ID = 5000-1FE1-0000-4252
```

```
PORT_2_TOPOLOGY = FABRIC (fabric up)
Address          = 200413
REMOTE_COPY     = BUILDNGB
```

```
.
.
.
```

3. If you changed an asynchronous remote copy set to synchronous during failover, change it back to asynchronous mode by issuing the following CLI command:

```
SET RemoteCopySetName OPERATION_MODE = ASYNCHRONOUS
```

Example: set rcs1 operation_mode = asynchronous

Repeat this step for all applicable remote copy sets.

4. Add back the target to the initiator unit's remote copy sets with the following CLI command:

```
SET RemoteCopySetName ADD = InitiatorRemoteCopyName\UnitName
```

Example: set rcs1 add = buildngA\d1

You will see a confirmation message, as shown in Example Display 15.

Example Display 15

```
BuildngBTop> set rcs1 add=buildngA\d1
```

```
%EVL--BuildngBTop> --10-MAY-2001 17:37:27-- Instance Code: 0E050064
Template: 144.(90)
```

```
.
.
.
```

```
Instance Code: 0E050064
```

Repeat this step for all remote copy sets.

NOTE: This command will cause the remote copy sets to begin normalization.

5. Enter the following command to see the percentage of normalization completion.

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to that in Example Display 16.

Example Display 16

```
BuildngBTop> show remote_copy_sets full
Name                               Uses                               Used by
-----
RCS1      remote copy                  D1                               AS_D1
Reported LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0134
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGB\D1) state:
  ONLINE to the other controller
Target state:
  BUILDNGB\D1      is COPYING                               94% complete
BuildngBTop> show remote_copy_sets full
Name                               Uses                               Used by
-----
RCS1      remote copy                  D1                               AS_D1
Reported LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0134
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGB\D1) state:
  ONLINE to the other controller
Target state:
  BUILDNGB\D1      is NORMAL
```

IMPORTANT: Wait for normalization on all remote copy sets to complete before you proceed.

When the units are all normalized, the Target state field of the display will show NORMAL.

- 6. If you plan to leave load running, you may now add write history logging to your association sets.

NOTE: For information on how to add write history logging to association sets, see Appendix C.

- 7. If you plan to leave load running, set failsafe mode with the following CLI command:

```
SET RemoteCopySetName ERROR_MODE = FAILSAFE
```

```
Example: set rcs1 error_mode = failsafe
```

NOTE: Failsafe mode cannot be set if the remote copy set is in an association set that will be used for write history logging.

- 8. When you are ready to resume the failback process, continue with the following steps.
- 9. Stop I/O from the target hosts to the remote copy set units.

- ① 10. Disable host access to the remote copy set units with the following CLI command:

```
SET UnitName DISABLE = TargetHostConnectionNamex,
TargetHostConnectionNamey
```

Example: set d1 disable = hostb1,hostb2

- ① 11. Verify the lack of host access by entering the following CLI command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 17. Note that connections to HostB1 and HostB2 are missing from the Access field.

Example Display 17

```
BuildngBTop> show units full
-----
LUN                               Uses                               Used by
-----
D1                                DISK10000                          BUILDNGB\RCS1
LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003E
NOIDENTIFIER
Switches:
  RUN                               NOWRITE_PROTECT                     READ_CACHE
  READAHEAD_CACHE                   WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD
State:
  ONLINE to the other controller
  PREFERRED_PATH = THIS_CONTROLLER
Size: 17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )

D2                                DISK20000                          BUILDNGA\RCS2
LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0135
NOIDENTIFIER
Switches:
  RUN                               NOWRITE_PROTECT                     READ_CACHE
  READAHEAD_CACHE                   WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  BUILDNGBA, BUILDNGBB, BUILDNGBC, BUILDNGBD
State:
  ONLINE to the other controller
  PREFERRED_PATH = OTHER_CONTROLLER
Size: 17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
```

Repeat this step for all units.

- ① 12. Continue with Full Failback at the initiator site with the Initiator Site Return Control Procedure.

Initiator Site Return Control Procedure

This section describes how to return Data Replication Manager control to the initiator site.

- ▶ 1. Disconnect controller access with the following CLI commands:

```
SET THIS_CONTROLLER PORT_2_TOPOLOGY = OFFLINE
SET OTHER_CONTROLLER PORT_2_TOPOLOGY = OFFLINE
```

- ▶ 2. Verify that controller access has been disconnected with the following CLI commands:

```
SHOW THIS_CONTROLLER
SHOW OTHER_CONTROLLER
```

You will see a display similar to that in Example Display 18.

Example Display 18

```
BuildngATop> show this_controller
Controller:
    HSG80 ZG84906303 Software V86-1P, Hardware E03
    NODE_ID           = 5000-1FE1-0000-01F0
    ALLOCATION_CLASS   = 0
    SCSI_VERSION      = SCSI-3
    Configured for MULTIBUS_FAILOVER with ZG84906237
        In dual-redundant configuration
    Device Port SCSI address 7
    Time: 10-MAY-2001 17:55:29
    Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
    Reported PORT_ID = 5000-1FE1-0000-01F3
    PORT_1_TOPOLOGY = FABRIC (fabric up)
    Address          = 220213
Host PORT_2:
    Reported PORT_ID = 5000-1FE1-0000-01F4
    PORT_2_TOPOLOGY = OFFLINE (offline)
    REMOTE_COPY = BUILDNGA
.
.
BuildngATop> show other_controller
Controller:
    HSG80 ZG84906237 Software V86-1P, Hardware E03
    NODE_ID           = 5000-1FE1-0000-01F0
    ALLOCATION_CLASS   = 0
    SCSI_VERSION      = SCSI-3
    Configured for MULTIBUS_FAILOVER with ZG84906303
        In dual-redundant configuration
    Device Port SCSI address 6
    Time: 10-MAY-2001 17:55:39
    Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
    Reported PORT_ID = 5000-1FE1-0000-01F1
    PORT_1_TOPOLOGY = FABRIC (fabric up)
```

```
Address = 250213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-01F2
  PORT_2_TOPOLOGY = OFFLINE (offline)
  REMOTE_COPY = BUILDNGA
.
.
.
```

- ▶ 3. Move the initiator role to the original initiator with the following CLI command:

```
SITE_FAILOVER TargetRemoteCopyName\RemoteCopySetName
```

Example: `site_failover buildngB\rsc1`

You will see a confirmation message, as shown in Example Display 19.

Example Display 19

```
%EVL--BuildngATop> --10-MAY-2001 17:57:17-- Instance Code: 0E010064
Template: 144.(90)
.
.
.
Instance Code: 0E010064
```

Repeat this step for each remote copy set.

- ▶ 4. Continue with Full Failback at the target site with the Target Site Restore Procedure.

Target Site Restore Procedure

- ⦿ 1. Write history logging must be disabled to delete association sets. Turn off write history logging, if enabled, with the following CLI command:

```
SET AssociationSetName NOLOG_UNIT
```

Example: `set as_d1 nolog_unit`

Repeat this procedure for each association set.

- ⦿ 2. Delete any association sets with the following CLI command:

```
DELETE AssociationSetName
```

Example: `delete as_d1`

Repeat this procedure for each association set.

- ⦿ 3. Delete all remote copy sets with following CLI command:

```
DELETE RemoteCopySetName
```

Example: `delete rsc1`

You will see a confirmation message, as shown in Example Display 20.

Example Display 20

```
BuildngBTop> delete rcs1
%EVL--BuildngBTop> --10-MAY-2001 18:01:12-- Instance Code: 0E020064
Template: 144.(90)
.
.
Instance Code: 0E020064
```

Repeat this step for each remote copy set.

- ④ 4. Set the maximum cached transfer size to 128 with the following CLI command:

```
SET UnitName MAXIMUM_CACHED_TRANSFER_SIZE = 128
Example: set d1 maximum_cached_transfer_size = 128
```

Repeat this step for each remote copy set unit.

NOTE: This command sets both the read and write maximum cached transfer size.

- ④ 5. Verify that maximum cached transfer size for each remote copy set unit is set to 128 by entering the following CLI command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 21.

Example Display 21

```
BuildngBTop> show units full
-----
```

LUN	Uses	Used by
D1	DISK10000	
LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003E		
NOIDENTIFIER		
Switches:		
RUN	NOWRITE_PROTECT	READ_CACHE
READAHEAD_CACHE	WRITEBACK_CACHE	
MAX_READ_CACHED_TRANSFER_SIZE = 128		
MAX_WRITE_CACHED_TRANSFER_SIZE = 128		
Access:		
BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD		
State:		
ONLINE to this controller		
Not reserved		
PREFERRED_PATH = THIS_CONTROLLER		
Size: 17769177 blocks		
Geometry (C/H/S): (5258 / 20 / 169)		
D2	DISK20000	
LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003F		
NOIDENTIFIER		
Switches:		
RUN	NOWRITE_PROTECT	READ_CACHE

```
READAHEAD_CACHE          WRITEBACK_CACHE
MAX_READ_CACHED_TRANSFER_SIZE = 128
MAX_WRITE_CACHED_TRANSFER_SIZE = 128
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD
State:
  ONLINE to the other controller
  PREFERRED_PATH = OTHER_CONTROLLER
Size:          17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
```

6. Continue with Full Failback at the initiator site with the Initiator Site Restoration of Target Connections Procedure.

Initiator Site Restoration of Target Connections Procedure

This section describes how to restore all target connections from the initiator site.

1. To restore the connections to the target site, enter the following CLI commands:

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

You will see a confirmation message, as shown in Example Display 22.

Example Display 22

```
%EVL--BuildngATop> --10-MAY-2001 18:05:11-- Instance Code: 0E120064
Template: 144.(90)
.
.
.
Instance Code: 0E120064
```

2. Verify that the connections have been restored with the following commands:

```
SHOW THIS_CONTROLLER
SHOW OTHER_CONTROLLER
```

You will see a display similar to that in Example Display 23.

Example Display 23

```
BuildngATop> show this_controller
Controller:
  HSG80 ZG84906303 Software V86-1P, Hardware E03
  NODE_ID          = 5000-1FE1-0000-01F0
  ALLOCATION_CLASS  = 0
  SCSI_VERSION     = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG84906237
  In dual-redundant configuration
  Device Port SCSI address 7
  Time: 10-MAY-2001 18:05:38
  Command Console LUN is lun 0 (NOIDENTIFIER)
```

```

Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-01F3
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address          = 220213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-01F4
  PORT_2_TOPOLOGY = FABRIC (fabric up)
  Address          = 220413
  REMOTE_COPY     = BUILDNGA
.
.
.
BuildngATop> show other_controller
Controller:
  HSG80 ZG84906237 Software V86-1P, Hardware E03
  NODE_ID          = 5000-1FE1-0000-01F0
  ALLOCATION_CLASS = 0
  SCSI_VERSION    = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG84906303
  In dual-redundant configuration
  Device Port SCSI address 6
  Time: 10-MAY-2001 18:05:48
  Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-01F1
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address          = 250213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-01F2
  PORT_2_TOPOLOGY = FABRIC (fabric up)
  Address          = 250413
  REMOTE_COPY     = BUILDNGA
.
.
.

```

- ▶ 3. Re-enable failsafe mode, if desired. To set failsafe mode, enter the following CLI command:

```
SET RemoteCopySetName ERROR_MODE = FAILSAFE
```

Example: set rcs1 error_mode = failsafe

NOTE: Failsafe cannot be set if the remote copy set is in an association set has a write history log attached.

- ▶ 4. If you changed an asynchronous remote copy set to synchronous during failover, change it back to asynchronous mode with the following CLI command:

```
SET RemoteCopySetName OPERATION_MODE = ASYNCHRONOUS
```

Example: set rcs1 operation_mode = asynchronous

Repeat this step for all applicable remote copy sets.

- ▶ 5. Create association sets and then add the log unit, if desired. For information on how to create association sets, with or without write history logging, see Appendix C.

IMPORTANT: If you will be using scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention (remote copy sets, stripesets, mirrorsets, RAIDsets, association sets, and connections)—use underscores instead. Dashes are not allowed by the Perl scripting language.

- ▶ 6. Enable host access to all units with the following CLI command:

```
SET UnitName ENABLE = InitiatorHostConnectionNamex,
InitiatorHostConnectionNamey
```

Example: set d1 enable = hosta1,hosta2

- ▶ 7. Verify that you have enabled host access with the following CLI command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 24.

Example Display 24

```
BuildngATop> show units full
```

LUN	Uses	Used by
D1	DISK10000	BUILDNGA\RCS1
LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0134 NOIDENTIFIER Switches: RUN NOWRITE_PROTECT READ_CACHE READAHEAD_CACHE WRITEBACK_CACHE MAX_READ_CACHED_TRANSFER_SIZE = 128 MAX_WRITE_CACHED_TRANSFER_SIZE = 128 Access: BUILDNGBA, BUILDNGBB, BUILDNGBC, BUILDNGBD, HOSTA1, HOSTA2 State: ONLINE to the other controller PREFERRED_PATH = THIS_CONTROLLER Size: 17769177 blocks Geometry (C/H/S): (5258 / 20 / 169)		
D2	DISK20000	BUILDNGA\RCS2
LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0135 NOIDENTIFIER Switches: RUN NOWRITE_PROTECT READ_CACHE READAHEAD_CACHE WRITEBACK_CACHE MAX_READ_CACHED_TRANSFER_SIZE = 128 MAX_WRITE_CACHED_TRANSFER_SIZE = 128 Access: BUILDNGBA, BUILDNGBB, BUILDNGBC, BUILDNGBD HOST A1, HOSTA2 State: ONLINE to the other controller PREFERRED_PATH = OTHER_CONTROLLER Size: 17769177 blocks Geometry (C/H/S): (5258 / 20 / 169)		

- ▶ 8. Set maximum cached transfer size to the original value using the following CLI command:

```
SET UnitName MAXIMUM_CACHED_TRANSFER_SIZE = InitiatorValue
```

```
Example: set d1 maximum_cache_transfer_size = 32
```

NOTE: The default setting for maximum_cache_transfer_size is 32.

- ▶ 9. Verify that the maximum cached transfer size was set correctly with this command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 25.

Example Display 25

```
BuildngATop> show units full
-----
```

LUN	Uses	Used by
D1	DISK10000	BUILDNGA\RCS1
LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0134 NOIDENTIFIER Switches: RUN NOWRITE_PROTECT READ_CACHE READAHEAD_CACHE WRITEBACK_CACHE MAX_READ_CACHED_TRANSFER_SIZE = 32 MAX_WRITE_CACHED_TRANSFER_SIZE = 32 Access: BUILDNGBA, BUILDNGBB, BUILDNGBC, BUILDNGBD, HOSTA1, HOSTA2 State: ONLINE to the other controller PREFERRED_PATH = THIS_CONTROLLER Size: 17769177 blocks Geometry (C/H/S): (5258 / 20 / 169)		
D2	DISK20000	
LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0135 NOIDENTIFIER Switches: RUN NOWRITE_PROTECT READ_CACHE READAHEAD_CACHE WRITEBACK_CACHE MAX_READ_CACHED_TRANSFER_SIZE = 32 MAX_WRITE_CACHED_TRANSFER_SIZE = 32 Access: BUILDNGBA, BUILDNGBB, BUILDNGBC, BUILDNGBD HOSTA1, HOSTA2 State: ONLINE to the other controller PREFERRED_PATH = OTHER_CONTROLLER Size: 17769177 blocks Geometry (C/H/S): (5258 / 20 / 169)		

- ▶ 10. Allow hosts to recognize new units. Follow the steps listed below for each operating system in your heterogeneous configuration:

- a. **Compaq OpenVMS:** If the initiator site hosts are shut down, boot them now. Booting the hosts enables OpenVMS to recognize the drives.

If the initiator site hosts are not shut down, use the following command from a privileged account to enable OpenVMS to recognize the drives:

```
MCR SYSMAN IO AUTOCONFIGURE/LOG
```

Mount the volumes associated with the remote copy set LUNs on each host with access to those LUNs.

- b. **Compaq Tru64 UNIX:** If the initiator site hosts are shut down, boot them now. Booting the hosts enables Tru64 UNIX to recognize the drives.

If the initiator site hosts are not shut down, use the following command to recognize the drives:

```
hwmgr - scan scsi
```

This might take a while for large configurations. If this is the case, scan only those SCSI buses that have new units added. Scan only one bus at a time. Use the following command:

```
hwmgr -scan scsi -bus x
```

where x is the SCSI bus number.

- c. **HP-UX:** If the initiator site hosts are shut down, boot them now. Booting the hosts enables HP-UX to recognize the drives.

If the initiator site hosts are not shut down, use the following commands to recognize the drives and mount the file systems:

```
ioscan -fnCdisk
```

```
mount -a
```

- d. **IBM AIX:** If the initiator site hosts are shut down, boot them now. Booting the hosts enables IBM AIX to recognize the drives.

If the initiator site hosts are not shut down, use the following commands to recognize the drives and mount the file systems:

```
cfgmgr -v
```

```
mount all
```

- e. **Microsoft Windows NT-X86:** Turn on or reboot the hosts at the initiator site and log in using an account that has administrative privileges. You should be able to see all of the units by choosing **My Computer**.
- f. **Microsoft Windows 2000:**
 - 1) If you *have not* changed the UNIT_OFFSET of any host connections since the hosts have been booted, you do not need to reboot the initiator site hosts.
 - a) On each host, log in using an account that has administrative privileges.
 - b) Open **Computer Management** and click **Disk Management**.
 - c) After **Disk Management** has initialized, go to the **Action** menu and click **Rescan Disks**. All of the failed over units should appear in the right-hand pane. If Secure Path is not installed correctly, you will see each unit twice.
 - 2) If you *have* changed the UNIT_OFFSET of any host connections, you must reboot that host. After the server has rebooted, log in using an account that has administrative privileges. You will see all of the units in **Computer Management > Disk Management**. If Secure Path is not installed correctly, you will see each drive twice.
- g. **Novell NetWare:** If the initiator site hosts are shut down, boot them now. Booting the hosts allows Novell NetWare to recognize the drives.

If the initiator site hosts are already up and running, or if they do not recognize the drives, issue the following command from the console before mounting the volumes:

```
SCAN FOR NEW DEVICES
```

Alternatively, you can use the `NWCONFIG` utility to issue this same command.

- h. **SUN Solaris:** Turn on or reboot the hosts using the command `reboot -- -r` at the initiator site and log in using an account that has administrative privileges. You should be able to see all of the units by using the `format` command.

If Secure Path was not configured for these units, you will not see the drives. You will need to edit the WWLIDs in the file `/kernel/drv/ldLite.conf`. To find the new WWLIDs of the units, use the `SHOW Unitname` command on the controller. You may also need to adjust the files `/kernel/drv/mda.conf` and `/kernel/drv/sd.conf` to accommodate the extras LUNs. When you have edited

ldLite.conf, *mda.conf*, and *sd.conf*, reboot the host using the `reboot -- -r` command. You should now be able to see the drives using the `format` command. Refer to the *Compaq SANworks Secure Path for Sun Solaris Installation and Reference Guide* for additional assistance.

This completes the Unplanned Site Failover with Full Failback.

Resumption of Operations After Unplanned Loss of Target Site Procedure (Failsafe Mode)

In this situation you have experienced an unplanned loss of target site function due to failure of the intersite links or similar event such as loss of power at the target, loss of both target switches, and so on. The duration of the outage is unknown. The remote copy sets are in failsafe mode and host I/O is paused. You will remove the targets, then resume host I/O until the connection to the target site is re-established. When the remote copy set's error mode is in failsafe, and the connection to the target site is lost, host I/O is paused. This is because the remote copy set's initiator state becomes inoperative with the remote copy set unit in failsafe locked mode.

This chapter contains these procedures to resume initiator site processing after an unplanned communication loss while in failsafe mode. All of the steps in this procedure are performed from the initiator site:

- “Verification of Lost Connections Procedure” on page 3–2
- “Resumption of Host Access to Remote Copy Sets Procedure” on page 3–3
- “Resumption of Operations and Return to Failsafe Mode Procedure” on page 3–4

NOTE: In this chapter, *initiator* site procedure steps are identified by an arrow symbol ► in the margin. *Target* site procedure steps are identified by a target symbol ☉ in the margin.

NOTE: Some example displays illustrate confirmation messages with the event log symbol (%EVL) and an instance code. Compare the instance code in the example with the instance code you receive. If the numbers are the same, you have performed the previous command correctly and have achieved the desired results. Note that you will be able to see these screens only if you are working from the controller to which the LUNs are online. Refer to the Troubleshooting chapter for more information on instance codes and their meanings.

Example displays may also contain bold text to identify information that is the most pertinent in the example. In many cases, items shown in bold text will help you verify the results of a previous command.

Verification of Lost Connections Procedure

This procedure verifies the lost communication link between initiator and target.

- ▶ 1. Verify that the connection to the target site is lost and host I/O is paused. If you are connected to the initiator site controllers when connection to the target site is lost, you will see a confirmation message, as shown in Example Display 1.

Example Display 1

```
BuildngATop>
%EVL--BuildngATop> --06-JUN-2001 12:57:13-- Instance Code: 0E098901
Template: 144.(90)
  Occurred on 06-JUN-2001 at 12:57:13
.
.
.
Instance Code: 0E098901
%EVL--BuildngATop> --06-JUN-2001 12:57:14-- Instance Code: 02908901
Template: 81.(51)
  Occurred on 06-JUN-2001 at 12:57:13
.
.
.
Instance Code: 02908901
```

- ▶ 2. Verify that the remote copy set's initiator state is inoperative with the unit failsafe locked by issuing the following CLI command:

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a confirmation message, as shown in Example Display 2.

Example Display 2

```
BuildngATop> show remote_copy_sets full
Name                               Uses                               Used by
-----
RCS1      remote copy                       D1                               AS_D1
Reported LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003E
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = FAILSAFE
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGA\D1) state:
INOPERATIVE
Unit failsafe locked
Target state:
  BUILDNGB\D1      is COPYING                               0% complete
```

- ▶ 3. Continue the restore process with the Resumption of Host Access to Remote Copy Sets Procedure, which allows host access to the remote copy sets.

Resumption of Host Access to Remote Copy Sets Procedure

This procedure re-establishes the online status of the initiator site.

- ▶ 1. Use the following CLI command to resume host I/O at the initiator site:

```
SET RemoteCopySetName ERROR_MODE = NORMAL
```

You will see a confirmation message, as shown in Example Display 3.

Example Display 3

```
BuildngATop> set rcs1 error_mode = normal
%EVL--BuildngATop> --06-JUN-2001 13:02:13-- Instance Code: 0E088864
  Template: 144.(90)
  Occurred on 06-JUN-2001 at 13:02:13
  .
  .
  .
Instance Code: 0E088864
```

- ▶ 2. Remove the targets with the following CLI command:

```
SET RemoteCopySetName REMOVE = TargetRemoteCopyName\UnitNumber
```

Example: set rcs1 remove = buildngB\d1

You will see a confirmation message, as shown in Example Display 4.

Example Display 4

```
BuildngATop> set rcs1 remove = buildngB\d1
%EVL--BuildngATop> --10-MAY-2001 16:49:55-- Instance Code: 0E078A01
  Template: 144.(90)
  .
  .
  .
Instance Code: 0E078A01
```

- ▶ 3. Verify that you have removed the targets by entering the following CLI command:

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to that in Example Display 5.

Example Display 5

```
BuildngATop> show remote_copy_sets full
Name                               Uses                               Used by
-----
RCS1      remote copy                       D1
Reported LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0134
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGA\D1) state:
  ONLINE to the other controller
No targets
```

- ▶ 4. Resume applications for each operating system in your heterogeneous configuration
- ▶ 5. Continue the restore process with the Resumption of Operations and Return to Failsafe Mode Procedure, which verifies the re-established connection to the target site.

Resumption of Operations and Return to Failsafe Mode Procedure

This procedure ensures that replication of I/O to the target site is re-established.

- ▶ 1. When connection to the target site is back, you will see a confirmation message, as shown in Example Display 6.

Example Display 6

```
%EVL--BuildngATop> --21-JAN-1946 01:38:56-- Instance Code: 0258000A
Template: 81.(51)
Power On Time: 0. Years, 72. Days, 3. Hours, 15. Minutes, 34. Seconds
.
.
Instance Code: 0258000A
```

- ▶ 2. Add back the target unit to the remote copy sets with the following CLI command:

```
SET RemoteCopySetName ADD = TargetRemoteCopyName\UnitName
```

Example: set rcs1 add = buildngB\d1

You will see a confirmation message, as shown in Example Display 7.

Example Display 7

```
BuildngATop> set rcs1 add=buildngB\d1
%EVL--BuildngATop> --10-MAY-2001 17:37:27-- Instance Code: 0E050064
  Template: 144.(90)
  Occurred on 10-MAY-2001 at 17:37:27
  .
  .
  .
Instance Code: 0E050064
```

Repeat this step for all remote copy sets.

NOTE: This command will cause the remote copy sets to begin normalization.

- ▶ 3. Enter the following command to see the percentage of normalization completion for all remote copy sets.

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to that in Example Display 8.

Example Display 8

```
BuildngATop> show remote_copy_sets full
Name                                     Uses                                     Used by
-----
RCS1          remote copy                D1                                     AS_D1
Reported LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0134
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGA\D1) state:
  ONLINE to the other controller
Target state:
  BUILDNGB\D1      is COPYING                94% complete
BuildngATop> show remote_copy_sets full
Name                                     Uses                                     Used by
-----
RCS1          remote copy                D1                                     AS_D1
Reported LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0134
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGA\D1) state:
  ONLINE to the other controller
Target state:
  BUILDNGB\D1      is NORMAL
```

When the units are all normalized, the Target field of the display will show NORMAL.

IMPORTANT: Wait for normalization on all remote copy sets to complete before you proceed.

- ▶ 4. Return the remote copy set's error mode back to failsafe with the following CLI command:

```
SET RemoteCopySetName ERROR_MODE = FAILSAFE
```

- ▶ 5. Verify that the error mode is failsafe, that the initiator state is online, and that the target state is normal with the following CLI command:

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to that in Example Display 9.

Example Display 9

```
BuildngATop> show remote_copy_sets full
Name                               Uses                               Used by
-----
RCS1      remote copy                       D1                               AS_D1
Reported LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003E
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = FAILSAFE
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGA\D1) state:
ONLINE to this controller
Not reserved
Target state:
BUILDNGB\D1     is NORMAL
```

This completes the procedure for resuming initiator site processing after an unplanned communication loss while in failsafe mode.

Resumption of Operations After Unplanned Loss of Target Site Procedure (Normal Mode)

This situation is similar to the scenario in Chapter 3 in that you have experienced an unplanned loss of target site function due to failure of the intersite links, but the remote copy sets are in normal mode. The duration of the outage is unknown, but longer than can be accommodated with write history logging. You will allow host access to the remote copy sets, then resume operations.

This chapter contains these procedures to resume initiator site processing after an unplanned communication loss while in normal mode. All of the steps in this procedure are performed from the initiator site:

- “Verification of Lost Connections Procedure” on page 4–2
- “Resumption of Host Access to Remote Copy Sets Procedure” on page 4–2
- “Verification of Resumption of Operations Procedure” on page 4–4

NOTE: In this chapter, *initiator* site procedure steps are identified by an arrow symbol ► in the margin. *Target* site procedure steps are identified by a target symbol ☉ in the margin.

NOTE: Some example displays illustrate confirmation messages with the event log symbol (%EVL) and an instance code. Compare the instance code in the example with the instance code you receive. If the numbers are the same, you have performed the previous command correctly and have achieved the desired results. Note that you will be able to see these screens only if you are working from the controller to which the LUNs are online. Refer to the Troubleshooting chapter for more information on instance codes and their meanings.

Example displays may also contain bold text to identify information that is the most pertinent in the example. In many cases, items shown in bold text will help you verify the results of a previous command.

Verification of Lost Connections Procedure

This procedure verifies the lost communication link between initiator and target.

- ▶ 1. Verify that the connection to the target site is lost. If you are connected to the initiator site controllers when connection to the target site is lost, you will see a confirmation message, as shown in Example Display 1.

Example Display 1

```
BuildngATop>
%EVL--BuildngATop> --06-JUN-2001 12:57:13-- Instance Code: 0E0F8B01
Template: 144.(90)
  Occurred on 06-JUN-2001 at 12:57:13
  .
  .
Instance Code: 0E098901
```

- ▶ 2. Continue the restore process with the Resumption of Host Access to Remote Copy Sets Procedure, which allows host access to the remote copy sets.

Resumption of Host Access to Remote Copy Sets Procedure

This procedure re-establishes the online status of the initiator site.

- ▶ 1. Determine which controller your remote copy set LUN is online to with the following CLI command. This is important because the command in step 2 to remove the LUN must be issued from the controller that the LUN is online to.

```
SHOW RemoteCopySetName
```

```
Example: show rcs1
```

You will see a display similar to that in Example Display 2.

Example Display 2

```
BuildngATop> show rcs1
Name                                     Uses                               Used by
-----
RCS1          remote copy                               D1
Reported LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0134
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGB\D1) state:
ONLINE to this controller
Target state:
BUILDNGB\D1      is NORMAL
```

- ▶ 2. If necessary, move to the controller that the remote copy set LUN is online to.
- ▶ 3. Remove the remote copy set LUN with the following CLI command:

```
SET RemoteCopySetName REMOVE = TargetRemoteCopyName\UnitNumber
```

Example: set rcs1 remove = buildngB\d1

You will see a confirmation message, as shown in Example Display 3.

Example Display 3

```
BuildngATop> set rcs1 remove = buildngB\d1
%EVL--BuildngATop> --10-MAY-2001 16:49:55-- Instance Code: 0E078A01
  Template: 144.(90)
  .
  .
  .
Instance Code: 0E078A01
```

- ▶ 4. Verify that you have removed the targets by entering the following CLI command:

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to that in Example Display 4.

Example Display 4

```
BuildngATop> show remote_copy_sets full
Name                               Uses          Used by
-----
RCS1      remote copy                    D1
Reported LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0134
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGB\D1) state:
  ONLINE to the other controller
No targets
```

- ▶ 5. Continue the restore process with the Verification of Resumption of Operations Procedure, which verifies the re-established connection to the target site.

Verification of Resumption of Operations Procedure

This procedure ensures that I/O to the target site is re-established.

- ▶ 1. When connection to the target site is back, you will see a confirmation message, as shown in Example Display 5.

Example Display 5

```
%EVL--BuildngATop> --21-JAN-1946 01:38:56-- Instance Code: 0E030064
Template: 81.(51)
.
.
Instance Code: 0258000A
```

- ▶ 2. Add back the target unit to the remote copy sets with the following CLI command:

```
SET RemoteCopySetName ADD = TargetRemoteCopyName\UnitName
Example: set rcs1 add = buildingB\d1
```

You will see a confirmation message, as shown in Example Display 6.

Example Display 6

```
BuildngATop> set rcs1 add = buildngB\d1
%EVL--BuildngBTop> --10-MAY-2001 17:37:27-- Instance Code: 0E050064
Template: 144.(90)
.
.
Instance Code: 0E050064
```

Repeat this step for all remote copy sets.

NOTE: This command will cause the remote copy sets to begin normalization.

3. Enter the following command to see the percentage of normalization completion for all remote copy sets.

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to that in Example Display 7.

Example Display 7

```
BuildngATop> show remote_copy_sets full
Name                               Uses                               Used by
-----
RCS1      remote copy                    D1                               AS_D1
Reported LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0134
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGA\D1) state:
  ONLINE to the other controller
Target state:
  BUILDNGB\D1      is COPYING                               94% complete

BuildngBTop> show remote_copy_sets full
Name                               Uses                               Used by
-----
RCS1      remote copy                    D1                               AS_D1
Reported LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0134
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGA\D1) state:
  ONLINE to the other controller
Target state:
  BUILDNGB\D1      is NORMAL
```

When the units are all normalized, the Target field of the display will show NORMAL.

IMPORTANT: Wait for normalization on all remote copy sets to complete before you proceed.

- ▶ 4. Verify that the error mode is set to normal, that the initiator state is online, and that the target state is normal, with the following CLI command:

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to that in Example Display 8.

Example Display 8

```
BuildngATop> show remote_copy_sets full
Name                               Uses                               Used by
-----
RCS1      remote copy                    D1                               AS_D1
Reported LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003E
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE = NORMAL
  FAILOVER_MODE = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGA\D1) state:
  ONLINE to this controller
  Not reserved
Target state:
  BUILDNGB\D1      is NORMAL
```

This completes the procedure for resuming initiator site processing after an unplanned communication loss while in normal mode.

Short Planned Site Failover with Fast Failback Procedure

You are planning on performing scheduled maintenance at the initiator site. The maintenance will be completed within a relatively short period of time (within several hours).

You will perform a failover to the target site. Because of the short duration of the planned outage, the write history log will be able to accommodate the accumulated writes. When the initiator is operational and back online, you will perform a fast failback to the initiator with the merge function.

This chapter contains these procedures to ensure that failover and subsequent failback during short duration maintenance at the initiator site function properly:

- “Power Up and Power Down” on page 5–1
- “Planned Site Failover” on page 5–2
- “Fast Failback” on page 5–19

NOTE: In this chapter, *initiator* site procedure steps are identified by an arrow symbol ► in the margin. *Target* site procedure steps are identified by a target symbol ☉ in the margin.

NOTE: Some example displays illustrate confirmation messages with the event log symbol (%EVL) and an instance code. Compare the instance code in the example with the instance code you receive. If the numbers are the same, you have performed the previous command correctly and have achieved the desired results. Note that you will be able to see these screens only if you are working from the controller to which the LUNs are online. Refer to the Troubleshooting chapter for more information on instance codes and their meanings.

Example displays may also contain bold text to identify information that is the most pertinent in the example. In many cases, items shown in bold text will help you verify the results of a previous command.

Power Up and Power Down

If you need to power up or power down your DRM system, follow the instructions in Appendix B.

Planned Site Failover

To carry out a planned failover, follow the procedure outlined in this chapter, in conjunction with a fast failback. A planned failover consists of the following procedures:

- Initiator Site Preparation Procedure
- Target Site Failover Procedure
- Target Host Setup Procedure

Initiator Site Preparation Procedure

- ▶ 1. Before performing the failover procedure, locate your record of SHOW command output that details the current initiator configuration. Verify that your target controller configuration is the same as your initiator controller configuration. Compare the status of the controllers, association sets, remote copy sets, units, and connections. Appendix A contains the full procedure.
- ▶ 2. Verify that all remote copy sets are in normal error mode by issuing the following command:

```
SHOW REMOTE_COPY_SETS FULL
```

The output shows the status of remote copy sets.

You will see a display similar to that in Example Display 1.

Example Display 1

```
BuildngATop> SHOW REMOTE_COPY_SETS FULL
Name                               Uses                               Used by
-----
RCS1      remote copy                       D1                               AS_D1
Reported LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0134
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGA\D1) state:
  ONLINE to this controller
  Not reserved
Target state:
  BUILDNGB\D1    is NORMAL
RCS2      remote copy                       D2
Reported LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0135
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
```

```
FAILOVER_MODE = MANUAL
OUTSTANDING_IOS = 20
Initiator (BUILDNGA\D2) state:
  ONLINE to this controller
  Not reserved
Target state:
  BUILDNGB\D2 is NORMAL
```

- ▶ 3. Follow the steps listed below for each operating system in your heterogeneous configuration:
- a. **Compaq OpenVMS:** If the operating system is up and running, and is being used exclusively for DRM operations, shut down the operating system and power off the hosts. If the operating system is being used for other applications, remove all I/O to the remote copy set LUNs that will be failed over, then dismount the volumes associated with these LUNs.
 - b. **Compaq Tru64 UNIX:** If the operating system is up and running and is being used exclusively for DRM operations, shut down the operating system and power off the hosts. If the operating system is being used for other applications, remove all I/O and unmount all file system LUNs that have remote copy sets that will be failed over.
 - c. **HP-UX:** If the operating system is up and running, remove all I/O to the remote copy set LUNs that will be failed over, then unmount the file systems associated with these LUNs.
 - d. **IBM AIX:** If the operating system is up and running, remove all I/O to the remote copy set LUNs that will be failed over, then unmount the file systems associated with these LUNs.
 - e. **Microsoft Windows NT-X86:** If the operating system is up and running, shut it down and power off the hosts.
 - f. **Microsoft Windows 2000:** If the operating system is up and running, shut it down and power off the hosts.
 - g. **Novell NetWare:** If the operating system is up and running, remove all I/O to the remote copy set LUNs that will be failed over, then dismount the volumes associated with these LUNs.

If you are using NetWare Cluster Services (NWCS), you must enter the `cluster down` command. You must also enter the `uldncs` (unload NetWare Cluster Services) command for all cluster nodes.

You will see a display similar to that in Example Display 2.

Example Display 2

```
BuildngATop> SHOW UNITS FULL
LUN                                     Uses                               Used by
-----
D1                                     DISK10000                          BUILDNGA\RCS1
LUN ID:                               6000-1FE1-0000-01F0-0009-8490-6303-0134
NOIDENTIFIER
Switches:
  RUN                                   NOWRITE_PROTECT                     READ_CACHE
  READAHEAD_CACHE                     WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  BUILDNGBA, BUILDNGBB, BUILDNGBC, BUILDNGBD
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = THIS_CONTROLLER
Size:                                  17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )

D2                                     DISK20000                          BUILDNGA\RCS2
LUN ID:                               6000-1FE1-0000-01F0-0009-8490-6303-0135
NOIDENTIFIER
Switches:
  RUN                                   NOWRITE_PROTECT                     READ_CACHE
  READAHEAD_CACHE                     WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  BUILDNGBA, BUILDNGBB, BUILDNGBC, BUILDNGBD
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = OTHER_CONTROLLER
Size:                                  17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
```

- b. If access to the target site controllers is not currently enabled, enable access by issuing the following command for each applicable remote copy set unit:

```
SET UnitName ENABLE = TargetRemoteCopyNameA,
TargetRemoteCopyNameB, TargetRemoteCopyNameC,
TargetRemoteCopyNameD
```

Example: set d1 enable = buildngbA,buildngbB,buildngbC, buildngbD

- ▶ 9. Set maximum cached transfer size to 128 with the following CLI command:

```
SET UnitName MAXIMUM_CACHED_TRANSFER_SIZE = 128
```

Example: set d1 maximum_cached_transfer_size = 128

Repeat this step for all units.

NOTE: This command sets both the read and write maximum cached transfer size.

- ▶ 10. Continue the failover process at the target site with the Target Site Failover Procedure.

Target Site Failover Procedure

- ⦿ 1. At the target site, the units must be preferred to one controller or the other.
 - a. Use the following CLI command to check for the preferred path:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 3.

Example Display 3

```
BuildngBTop> SHOW UNITS FULL
-----
LUN                               Uses                               Used by
-----
D1                                  DISK10000                          BUILDNGA\RCS1
LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003E
NOIDENTIFIER
Switches:
  RUN                               NOWRITE_PROTECT                     READ_CACHE
  READAHEAD_CACHE                  WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 128
  MAX_WRITE_CACHED_TRANSFER_SIZE = 128
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = THIS_CONTROLLER
  Target NORMAL
Size: 17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
D2                                  DISK20000                          BUILDNGA\RCS2
LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003F
NOIDENTIFIER
Switches:
  RUN                               NOWRITE_PROTECT                     READ_CACHE
  READAHEAD_CACHE                  WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 128
  MAX_WRITE_CACHED_TRANSFER_SIZE = 128
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = OTHER_CONTROLLER
  Target NORMAL
Size: 17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
```

- b. If units are not currently preferred, use the following CLI command:

```
SET UnitName PREFERRED_PATH = THIS_CONTROLLER
```

```
Example: set d1 preferred_path = this_controller
```

or

```
SET UnitName PREFERRED_PATH = OTHER_CONTROLLER
```

```
Example: set d2 preferred_path = other_controller
```

Repeat this step for each remote copy set unit that needs to be preferred.

2. Disconnect controller access with the following CLI commands:

```
SET THIS_CONTROLLER PORT_2_TOPOLOGY = OFFLINE
```

```
SET OTHER_CONTROLLER PORT_2_TOPOLOGY = OFFLINE
```

3. Verify controller access has been disconnected with the following CLI commands:

```
SHOW THIS_CONTROLLER
```

```
SHOW OTHER_CONTROLLER
```

You will see a display similar to that in Example Display 4.

Example Display 4

```
BuildngBTop> show this_controller
Controller:
  HSG80 ZG84906303 Software V86-1P, Hardware E03
  NODE_ID           = 5000-1FE1-0000-01F0
  ALLOCATION_CLASS   = 0
  SCSI_VERSION      = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG84906237
  In dual-redundant configuration
  Device Port SCSI address 7
  Time: 10-MAY-2001 17:55:29
  Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-01F3
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address          = 220213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-01F4
  PORT_2_TOPOLOGY = OFFLINE (offline)
  REMOTE_COPY = BUILDNGA
.
.
.
BuildngBTop> show other_controller
Controller:
  HSG80 ZG84906237 Software V86-1P, Hardware E03
  NODE_ID           = 5000-1FE1-0000-01F0
  ALLOCATION_CLASS   = 0
  SCSI_VERSION      = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG84906303
  In dual-redundant configuration
  Device Port SCSI address 6
```

```
Time: 10-MAY-2001 17:55:39
Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-01F1
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address          = 250213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-01F2
  PORT_2_TOPOLOGY = OFFLINE (offline)
  REMOTE_COPY     = BUILDNGA
.
.
.
```

4. Move the initiator role to the target controller with the following CLI command:

```
SITE_FAILOVER InitiatorRemoteCopyName\RemoteCopySetName
```

```
Example: site_failover buildnga\rctl
```

You will see a confirmation message, as shown in Example Display 5.

Example Display 5

```
BuildngBTop> site_failover Buildnga\rctl
%EVL--BuildngBTop> --10-MAY-2001 15:47:39-- Instance Code: 0E010064
Template: 144.(90)
.
.
.
Instance Code: 0E010064
```

Repeat this step for each remote copy set.

5. Restore the connections to the initiator site with the following CLI commands:

```
SET THIS_CONTROLLER PORT_2_TOPOLOGY = FABRIC
```

```
SET OTHER_CONTROLLER PORT_2_TOPOLOGY = FABRIC
```

6. Verify that connections have been restored by issuing the following CLI command:

```
SHOW THIS_CONTROLLER
```

```
SHOW OTHER_CONTROLLER
```

You will see a display similar to that in Example Display 6.

Example Display 6

```
BuildngBTop> show this_controller
Controller:
  HSG80 ZG94115654 Software V86-1P, Hardware E10
  NODE_ID          = 5000-1FE1-0000-4250
  ALLOCATION_CLASS  = 0
```



```

SCSI_VERSION      = SCSI-3
Configured for MULTIBUS_FAILOVER with ZG94319198
  In dual-redundant configuration
Device Port SCSI address 7
Time: 10-MAY-2001 17:34:11
Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-4253
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address          = 260213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-4254
  PORT_2_TOPOLOGY = FABRIC (fabric up)
  Address          = 260413
  REMOTE_COPY     = BUILDNGB
.
.
BuildngBTop> show other_controller
Controller:
  HSG80 ZG94319198 Software V86-1P, Hardware E10
  NODE_ID          = 5000-1FE1-0000-4250
  ALLOCATION_CLASS  = 0
  SCSI_VERSION     = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG94115654
  In dual-redundant configuration
  Device Port SCSI address 6
  Time: 10-MAY-2001 17:34:20
  Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-4251
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address          = 200213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-4252
  PORT_2_TOPOLOGY = FABRIC (fabric up)
  Address          = 200413
  REMOTE_COPY     = BUILDNGB
.
.

```

Create a Log Unit

1. If not already created during the target site setup procedure, create a mirrorset for the log disk by issuing the following CLI command:

```
ADD MIRRORSET MirrorsetName DiskName1 DiskName2
```

```
Example: add mirr mir_dllog disk50100 disk60100
```

IMPORTANT: If you will be using scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention (remote copy sets, stripesets, mirrorsets, RAIDsets, association sets, and connections)—use underscores instead. Dashes are not allowed by the Perl scripting language.

NOTE: To minimize the number of devices used for logging, you can create and use one-member mirrorsets. Because the data is written to one disk, the logged data will not be protected. However, all of this data is also written to the initiator unit. In the case of a log disk failure, you would incur a full normalization, rather than a mini-merge, when access to the target is re-established.

The command to create a one-member mirrorset is the same as above, except only one disk is listed.

Example: `add mirr mir_d11log disk50100`

- 2. Initialize the mirrorset with the following CLI command:

`INITIALIZE ContainerName`

Example: `initialize mir_d1log`

- 3. Verify that you have created a mirrorset by issuing the following CLI command:

`SHOW MIRRORSET`

You will see a display similar to that in Example Display 7.

Example Display 7

Name	Storageset	Uses	Used by
MIR_D1LOG	mirrorset	DISK50100 DISK60100	

- 4. Present the log unit to the controller with the following CLI command:

`ADD UNIT UnitName ContainerName`

Example: `add unit d10 mir_d1log`

- 5. Verify that the controller recognizes the log unit by issuing the following CLI command:

`SHOW UNITS`

You will see a display similar to that in Example Display 8.

Example Display 8

LUN	Uses	Used by
D10	MIR_D1LOG	

Create Association Sets and Assign a Log Unit

IMPORTANT: If you will be using scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention (remote copy sets, stripesets, mirrorsets, RAIDsets, association sets, and connections)—use underscores instead. Dashes are not allowed by the Perl scripting language.

1. Create an association set with the following CLI command:

```
ADD ASSOCIATIONS AssociationSetName RemoteCopySetName
```

Example: add associations as_d1 rcs1

Repeat this step for each association set.

NOTE: You can add additional members to the association set by issuing the following CLI command:

```
Set AssociationSetName ADD = RemoteCopySetName
```

Example: set as_d1 add = rcs1

2. Disable node access to the log unit with the following CLI command:

```
SET UnitNumber DISABLE_ACCESS_PATH = ALL
```

Example: set d10 disable_access_path = all

3. Disable writeback cache on log units with the following CLI command:

```
SET UnitNumber NOWRITEBACK_CACHE
```

Example: set d10 nowriteback_cache

4. Check to see that you have disabled access and writeback cache with the following command:

```
SHOW D10
```

You will see a display similar to that in Example Display 9.

Example Display 9

LUN	Uses	Used by
D10	MIR_D1LOG	
LUN ID:	6000-1FE1-0001-3B10-0009-9130-8044-0066	
IDENTIFIER =	10	
Switches:		
RUN	NOWRITE_PROTECT	READ_CACHE
READAHEAD_CACHE	NOWRITEBACK_CACHE	
MAXIMUM_CACHED_TRANSFER_SIZE =	32	
Access:		
None		
State:		
ONLINE to this controller		
Not reserved		

```
PREFERRED_PATH = THIS_CONTROLLER
Size:          35556389 blocks
Geometry (C/H/S): ( 7000 / 20 / 254 )
```

- 5. Assign the log units to the association sets with the following CLI command:

```
SET AssociationSetName LOG_UNIT = D10
```

Example: set as_d1 log_unit = d10

- 6. Check to see the switch status of the association set by issuing the following CLI command:

```
SHOW ASSOCIATIONS FULL
```

You will see a display similar to Example Display 10.

Example Display 10

```
BuildngBTop> show associations full
Name          Association          Uses          Used by
-----
AS_D1         association          RCS1
Switches:
  NOFAIL_ALL
  NOORDER_ALL
  LOG_UNIT = D10 (No data logged)
```

Repeat this step for each association set.

- 7. Continue the failover procedure at the target site with the Target Host Setup Procedure.

Target Host Setup Procedure

- 1. You can enhance host I/O performance by resetting the maximum cached transfer size to the value used on the initiator. Use this command:

```
SET UnitName MAXIMUM_CACHED_TRANSFER_SIZE = InitiatorValue
```

Example: set d1 maximum_cached_transfer_size = 32

Repeat this step for each unit.

NOTE: The default maximum cached transfer size is 32.

- 2. Suspend write operations to the target site with the CLI command.

```
SET RemoteCopySetName SUSPEND = TargetName\UnitName
```

Example: set rcs1 suspend = buildngb\d1

You will see a confirmation message, as shown in Example Display 11.

Example Display 11

```
%EVL--BuildngBTop> --07-JUN-2001 11:51:01-- Instance Code: 0E210064
Template: 144.(90)
.
.
Instance Code: 0E210064
```

Repeat this step for all remote copy sets.

3. Use the following CLI command to verify that the remote copy sets are suspended and that the log unit is available.

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to that in Example Display 12.

Example Display 12

```
BuildngBTop> SHOW REMOTE_COPY_SETS FULL
Name                               Uses                               Used by
-----
RCS1      remote copy                       D1                               AS_D1
Reported LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003E
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGB\D1) state:
  ONLINE to this controller
  Not reserved
Target state:
  BUILDNGA\D1      is SUSPENDED      LOG_UNIT 99% available
```

4. Give the target site hosts access to the units that are used by remote copy sets in the storage subsystems, with this command:

```
SET UnitName ENABLE = TargetHostConnectionNamex,
TargetHostConnectionNamey
```

Example: set d1 enable = hostb1,hostb2

You will see a display similar to that in Example Display 13.

Example Display 13

```
BuildngBTop> set d1 enable=hostb1,hostb2
Warning 1000: Other host(s) in addition to the one(s) specified can still
access this unit. If you wish to enable ONLY the host(s)
specified, disable all access paths (DISABLE_ACCESS=ALL), then
again enable the ones specified
```

- 5. After you have given the target site hosts access, verify the access with the following CLI command:

```
SHOW UNIT_NAME
```

You will see a display similar to that in Example Display 14.

Example Display 14

```
BuildngBTop> show d1
LUN                                     Uses                                Used by
-----
D1                                     DISK10000                           BUILDNGB\RCS1
LUN ID:                               6000-1FE1-0000-4250-0009-9411-5654-003E
NOIDENTIFIER
Switches:
  RUN                                  NOWRITE_PROTECT                       READ_CACHE
  READAHEAD_CACHE                     WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD,  HOSTB1,  HOSTB2
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = THIS_CONTROLLER
Size:                                  17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
```

Repeat this step for each unit.

- 6. If you do not recall a target host connection name, use the following command:

```
SHOW CONNECTION
```

You will see a display similar to that in Example Display 15.

Example Display 15

```
BuildngBTop> show connection
Connection
Name      Operating system  Controller  Port  Address  Status  Unit Offset
-----
BUILDNGAA  PPRC_TARGET      THIS       2     220413  offline 0
HOST_ID=5000-1FE1-0000-01F0 ADAPTER_ID=5000-1FE1-0000-01F4
BUILDNGAB  PPRC_TARGET      OTHER      2     250413  offline 0
HOST_ID=5000-1FE1-0000-01F0 ADAPTER_ID=5000-1FE1-0000-01F2
BUILDNGAC  PPRC_INITIATOR   THIS       2     220413  OL this 0
HOST_ID=5000-1FE1-0000-01F0 ADAPTER_ID=5000-1FE1-0000-01F4
BUILDNGAD  PPRC_INITIATOR   OTHER      2     250413  OL other 0
HOST_ID=5000-1FE1-0000-01F0 ADAPTER_ID=5000-1FE1-0000-01F2
HOSTA1     WINNT             THIS       1     260013  OL this 0
HOST_ID=1000-0000-C920-A7B9 ADAPTER_ID=1000-0000-C920-A7B9
```

HOSTA2	WINNT	OTHER	1	200013	OL other	0
HOST_ID=1000-0000-C921-3F4E		ADAPTER_ID=1000-0000-C921-3F4E				
HOSTB1	WINNT	THIS	1	220013	OL this	0
HOST_ID=1000-0000-C921-3E98		ADAPTER_ID=1000-0000-C921-3E98				
HOSTB2	WINNT	OTHER	1	250013	OL other	0
HOST_ID=1000-0000-C921-3EFC		ADAPTER_ID=1000-0000-C921-3EFC				

7. To verify that the previous steps have been completed successfully, issue this CLI command:

```
SHOW REMOTE_COPY_SETS FULL
```

The output shows the status of remote copy sets, as shown in Example Display 16.

Example Display 16

```
BuildngBTop> show remote_copy_sets full
Name                               Uses                               Used by
-----
RCS1      remote copy                    D1                               AS_D1
Reported LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0134
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGB\D1) state:
  ONLINE to this controller
  Not reserved
Target state:
  BUILDNGA\D1      is LOGGING          LOG_UNIT 99% available
```

NOTE: Be sure that the units you see (listed under Initiator state) are at the target site.

8. To verify that the target hosts can connect to the LUNs, use this command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 17.

Example Display 17

```
BuildngBTop> show units full
LUN                               Uses                               Used by
-----
D1                                 DISK10000                          BUILDNGB\RCS1
LUN ID:      6000-1FE1-0000-4250-0009-9411-5654-003E
NOIDENTIFIER
Switches:
  RUN                               NOWRITE_PROTECT                      READ_CACHE
  READAHEAD_CACHE                   WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
```

```

        BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD,      HOSTB1,      HOSTB2
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = THIS_CONTROLLER
Size:      17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
D2
        DISK20000                                BUILDNGA\RCS2
LUN ID:      6000-1FE1-0000-4250-0009-9411-5654-003F
NOIDENTIFIER
Switches:
  RUN                                NOWRITE_PROTECT                READ_CACHE
  READAHEAD_CACHE                    WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
        BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD,      HOSTB1,      HOSTB2
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = OTHER_CONTROLLER
  Target NORMAL
Size:      17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )

```

In the Access field of the display, all units that are used by remote copy sets will show that the target host connections are enabled. This will also show the initiator controller connections.

- 9. Allow hosts to recognize new units. Follow the steps listed below for each operating system in your heterogeneous configuration:

- a. **Compaq OpenVMS:** If the target site hosts are shut down, boot them now. Booting the hosts enables OpenVMS to recognize the drives.

If the target site hosts are not shut down, use the following command from a privileged account to enable OpenVMS to recognize the drives:

```
MCR SYSMAN IO AUTOCONFIGURE/LOG
```

- b. **Compaq Tru64 UNIX:** If the target site hosts are shut down, boot them now. Booting the hosts enables Tru64 UNIX to recognize the drives.

If the target site hosts are not shut down, use the following command to recognize the drives:

```
hwmgr - scan scsi
```

This might take a while for large configurations. If this is the case, scan only those SCSI buses that have new units added. Scan only one bus at a time. Use the following command:

```
hwmgr -scan scsi -bus x
```

where x is the SCSI bus number.

c. **HP-UX:**

- 1) If the target site hosts are shut down, boot them now. Booting the hosts enables HP-UX to recognize the drives.

If the target site hosts are not shut down, use the following command to enable HP-UX to recognize the drives and verify that they are present. This command will display only the previously configured failed-over LUNs:

```
ioscan -fnCdisk
```

- 2) Continue with the following commands to access file systems on new failed-over LUNs. If you have no new failed-over LUNs, skip these substeps and go directly to the next step to mount the LUNs:

- a. `/opt/CPQswsp/spmgr display -u`

- b. `/opt/CPQswsp/spmgr add WWN`

Repeat this command for each un-attached WWN that was displayed.

- c. `ioscan -fnCdisk`

If the device special files were not displayed, run `insf -e`, then run `ioscan -fnCdisk` again.

- d. `vgimport VolumeGroupName DeviceSpecialFile`

Repeat this command for each new failed-over LUN.

- 3) Use the following command to mount the LUNs:

```
mount -a
```

NOTE: *VolumeGroupName* is the name of the volume group you originally created at the initiator site. The *DeviceSpecialFiles* are from the `ioscan` in the form of `/dev/dsk/c_t_d_`.

For consistency, configure the same *DeviceSpecialFiles* with the same volume groups, logical volumes, and file systems for the failed-over LUNs at the target site with the same LUNs at the initiator site.

- d. **IBM AIX:** If the target site hosts are shut down, boot them now. Booting the hosts enables IBM AIX to recognize the drives.

If the target site hosts are not shut down, use the following commands to enable AIX to recognize the drives and verify that they are present:

```
cfgmgr -v
```

```
lsdev -Cc disk
```

Use the following commands to access file systems on the failed-over LUNs:

```
importvg -y volumegroupname hdiskx
mount all
```

NOTE: *volumegroupname* is the name of the volume group you originally created at the initiator site, and *x* is the number of the hdisk assigned to the failed-over LUN. If the *-y volumegroupname* parameter is omitted, AIX will create a default volume group name for you, for example, *vg00*.

- e. **Microsoft Windows NT-X86:** Reboot the hosts at the target site and log in using an account that has administrative privileges. You should be able to see all of the units by choosing **My Computer**.
- f. **Microsoft Windows 2000:**
 - 1) If you *have not* changed the UNIT_OFFSET of any host connections since the hosts have been booted, you do not need to reboot the initiator site hosts.
 - a) On each host, log in using an account that has administrative privileges.
 - b) Open **Computer Management** and click **Disk Management**.
 - c) After **Disk Management** has initialized, go to the **Action** menu and click **Rescan Disks**. All of the failed over units should appear in the right-hand pane. If Secure Path is not installed correctly, you will see each unit twice.
 - 2) If you *have* changed the UNIT_OFFSET of any host connections, you must reboot that host. After the server has rebooted, log in using an account that has administrative privileges. You will see all of the units in **Computer Management > Disk Management**. If Secure Path is not installed correctly, you will see each drive twice.
- g. **Novell NetWare:** If the target site hosts are shut down, boot them now. If you are using traditional NetWare volumes, booting the hosts allows Novell NetWare to recognize the drives and automatically mount the volumes. If you are using NSS logical volumes, booting the hosts will recognize the NSS pools and activate them. However, you must manually mount each individual NSS volume by typing `MOUNT VolumeName` at the NetWare console.

If the target site hosts are already up and running, or if they do not recognize the drives, issue the following command from the console before mounting the volumes:

```
SCAN FOR NEW DEVICES
```

Alternatively, you can use the `NWCONFIG` utility to issue this same command.

Next, mount the volumes with these commands:

```
MOUNT ALL (for traditional NetWare volumes)
```

```
MOUNT VolumeName (for NSS logical volumes).
```

- h. **SUN Solaris:** Reboot the hosts using the command `reboot -- -r` at the target site and log in using an account that has administrative privileges. You should be able to see all of the units by using the `format` command.

If Secure Path was not configured for these units, you will not see the drives. You will need to edit the WWLIDs in the file `/kernel/drv/ldLite.conf`. To find the new WWLIDs of the units, use the `SHOW Unitname` command on the controller. You may also need to adjust the files `/kernel/drv/mda.conf` and `/kernel/drv/sd.conf` to accommodate the extras LUNs. When you have edited `ldLite.conf`, `mda.conf`, and `sd.conf`, reboot the host using the `reboot -- -r` command. You should now be able to see the drives using the `format` command. Refer to the *Compaq SANworks Secure Path for Sun Solaris Installation and Reference Guide* for additional assistance.

This completes Planned Site Failover. Proceed with Fast Failback in the next section.

Fast Failback

Fast Failback is used in conjunction with Planned Site Failover. Before performing Fast Failback, locate your record of `SHOW` command output that details the initiator configuration. This is a planned event and is performed only after both initiator and target are synchronized.

Compare the status of the controllers, association sets, remote copy sets, units, and connections. Appendix A contains the full procedure. Verify that your target controller configuration is the same as your initiator controller configuration.

Fast Failback consists of the following procedures:

- Target Site Failback Procedure
- Initiator Site Cleanup Procedure

Target Site Failback Procedure

1. When the maintenance at the initiator site is complete, reconnect the targets.
2. Allow the write history log to merge with the following CLI command:

```
SET RemoteCopySetName RESUME = InitiatorName\UnitName
```

```
Example: set rcs1 resume = buildnga\d1
```

You will see a confirmation message, as shown in Example Display 18.

Example Display 18

```
%EVL--BuildngBTop> --07-JUN-2001 12:09:41-- Instance Code: 0E220064
Template: 144.(90)
.
.
Instance Code: 0E220064
```

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

3. Shut down the target site hosts (this is not necessary for Compaq OpenVMS, Compaq Tru64 UNIX, HP-UX, IBM AIX, Sun Solaris, and Novell Netware operating systems).

IMPORTANT: If hosts are not shut down, you must remove host access on all LUNs used with remote copy sets.

4. Disable host access to the target units for all remote copy sets with the following CLI command:

```
SET UnitName DISABLE = TargetHostConnectionNamex,
TargetHostConnectionNamey
```

```
Example: set d1 disable = hostb1,hostb2
```

Repeat this step for all units.

5. You may now boot hosts for non-remote copy set units.
6. Turn off write history logging, if enabled, with the following CLI command:

```
SET AssociationSetName NOLOG_UNIT
```

```
Example: set as_d1 nolog_unit
```

Repeat this procedure for each association set.

- ⑦ 7. Delete any association sets with the following CLI command:

```
DELETE AssociationSetName
```

Example: delete as_d1

Repeat this procedure for each association set.

- ⑧ 8. Move control of the remote copy sets to the original initiator with the following CLI command:

```
SET RemoteCopySetName INITIATOR = InitiatorRemoteCopyName\UnitName
```

Example: set rcs1 initiator = buildnga\d1

- ⑨ 9. Verify original initiator control with the following CLI command:

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to that in Example Display 19. The `NO REMOTE_COPY_SETS` display indicates that the original initiator has control.

Example Display 19

```
BuildngBTop> show remote_copy_sets full
No REMOTE_COPY_SETS
```

Repeat this step for all remote copy sets.

NOTE: If, after issuing this command for one of the remote copy sets, you get the error message: `Error: Rem Cp Set specified is currently in a transient state, wait a few seconds and try again.` The command will eventually succeed.

- ⑩ 10. If maximum cached transfer size was changed for the target units as part of the failover procedure, set it back to 128 with the following CLI command:

```
SET UnitName MAXIMUM_CACHED_TRANSFER_SIZE = 128
```

Example: set d1 maximum_cached_transfer_size = 128

- ⑪ 11. Verify that the maximum cached transfer size has been changed to 128 with the following CLI command:

```
SHOW UnitName
```

You will see a display similar to that in Example Display 20.

Example Display 20

```

BuildngBTop> show d1
LUN                               Uses                               Used by
-----
D1                                  DISK10000                          BUILDNGA\RCS1
LUN ID:        6000-1FE1-0000-4250-0009-9411-5654-003E
NOIDENTIFIER
Switches:
  RUN                               NOWRITE_PROTECT                      READ_CACHE
  READAHEAD_CACHE                   WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 128
  MAX_WRITE_CACHED_TRANSFER_SIZE = 128
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD
State:
  ONLINE to the other controller
  PREFERRED_PATH = THIS_CONTROLLER
  Target NORMAL
Size:          17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )

```

Repeat this procedure for each unit.

NOTE: This command sets both the read and write maximum cached transfer size.

- ② 12. Continue with the failback procedure at the initiator site with the Initiator Site Cleanup Procedure.

Initiator Site Cleanup Procedure

- ▶ 1. You can enhance host I/O performance by resetting the maximum cached transfer size to the original value used on the initiator. Use this command:

```
SET UnitName MAXIMUM_CACHED_TRANSFER_SIZE = InitiatorValue
```

Example: `set d1 maximum_cached_transfer_size = 32`

Repeat this step for all each unit.

- ▶ 2. Verify the above step with the following CLI command:

```
SHOW_UNITS_FULL
```

You will see a display similar to that in Example Display 21.

Example Display 21

```

BuildngATop> show units full
LUN                               Uses                               Used by
-----
D1                                  DISK10000                          BUILDNGA\RCS1
LUN ID:        6000-1FE1-0000-01F0-0009-8490-6303-0134
NOIDENTIFIER
Switches:

```

```

        RUN                NOWRITE_PROTECT        READ_CACHE
        READAHEAD_CACHE    WRITEBACK_CACHE
        MAX_READ_CACHED_TRANSFER_SIZE = 32
        MAX_WRITE_CACHED_TRANSFER_SIZE = 32
    Access:
        BUILDNGBA, BUILDNGBB, BUILDNGBC, BUILDNGBD
    State:
        ONLINE to the other controller
        PREFERRED_PATH = THIS_CONTROLLER
    Size:                17769177 blocks
    Geometry (C/H/S): ( 5258 / 20 / 169 )
D2                                DISK20000        BUILDNGA\RCS2
    LUN ID:                6000-1FE1-0000-01F0-0009-8490-6303-0135
    NOIDENTIFIER
    Switches:
        RUN                NOWRITE_PROTECT        READ_CACHE
        READAHEAD_CACHE    WRITEBACK_CACHE
        MAX_READ_CACHED_TRANSFER_SIZE = 32
        MAX_WRITE_CACHED_TRANSFER_SIZE = 32
    Access:
        BUILDNGBA, BUILDNGBB, BUILDNGBC, BUILDNGBD
    State:
        ONLINE to the other controller
        PREFERRED_PATH = OTHER_CONTROLLER
    Size:                17769177 blocks
    Geometry (C/H/S): ( 5258 / 20 / 169 )
D10                                MIR_DLOG
    LUN ID:                6000-1FE1-0000-01F0-0009-8490-6303-0181
    NOIDENTIFIER
    Switches:
        RUN                NOWRITE_PROTECT        READ_CACHE
        READAHEAD_CACHE    NOWRITEBACK_CACHE
        MAX_READ_CACHED_TRANSFER_SIZE = 32
        MAX_WRITE_CACHED_TRANSFER_SIZE = 32
    Access:
        None
    State:
        ONLINE to this controller
        Not reserved
        PREFERRED_PATH = THIS_CONTROLLER
    Size:                17769177 blocks
    Geometry (C/H/S): ( 5258 / 20 / 169 )

```

- ▶ 3. Create association sets and then add the log unit, if desired. For information on how to create association sets, with or without write history logging, see Appendix C.

IMPORTANT: If you will be using scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention (remote copy sets, stripesets, mirrorsets, RAIDsets, association sets, and connections)—use underscores instead. Dashes are not allowed by the Perl scripting language.

- ▶ 4. When you have created the association set, verify it with the following CLI command:

```
SHOW ASSOCIATION_SETS FULL
```

You will see a display similar to that in Example Display 22.

Example Display 22

```

BuildngATop> show as_d1
Name          Association          Uses          Used by
-----
AS_D1       association          RCS1
Switches:
NOFAIL_ALL
NOORDER_ALL
LOG_UNIT = D10 (No data logged)

```

- 5. If you changed an asynchronous remote copy set to synchronous during failover, change it back to asynchronous mode by issuing the following CLI command:

```
SET RemoteCopySetName OPERATION_MODE = ASYNCHRONOUS
```

Example: `set rcs1 operation_mode = asynchronous`

Repeat this step for all applicable remote copy sets.

- 6. Re-enable failsafe mode, if desired. To set failsafe mode, enter the following CLI command:

```
SET RemoteCopySetName ERROR_MODE = FAILSAFE
```

Example: `set rcs1 error_mode = failsafe`

Repeat this step for all applicable remote copy sets.

NOTE: Failsafe cannot be set if the remote copy set is in an association set that will be used for write history logging.

- 7. When you are ready to return to your original initiator, enable access to the initiator site host by using the following CLI command:

```
SET UnitName ENABLE = InitiatorHostConnectionNamex,
InitiatorHostConnectionNamey
```

Example: `set d1 enable = hosta1,hosta2`

- 8. Allow hosts to recognize new units. Follow the steps listed below for each operating system in your heterogeneous configuration:

- a. **Compaq OpenVMS:** If the initiator site hosts are shut down, boot them now. Booting the hosts enables OpenVMS to recognize the drives.

If the initiator site hosts are not shut down, use the following command from a privileged account to enable OpenVMS to recognize the drives:

```
MCR SYSMAN IO AUTOCONFIGURE/LOG
```

- b. **Compaq Tru64 UNIX:** If the initiator site hosts are shut down, boot them now. Booting the hosts enables Tru64 UNIX to recognize the drives.

If the initiator site hosts are not shut down, use the following command to recognize the drives:

```
hwmgr - scan scsi
```

This might take a while for large configurations. If this is the case, scan only those SCSI buses that have new units added. Scan only one bus at a time. Use the following command:

```
hwmgr -scan scsi -bus x
```

where x is the SCSI bus number.

- c. **HP-UX:** If the initiator site hosts are shut down, boot them now. Booting the hosts enables HP-UX to recognize the drives.

If the initiator site hosts are not shut down, use the following commands to recognize the drives and mount the file systems:

```
ioscan -fnCdisk
```

```
mount -a
```

- d. **IBM AIX:** If the initiator site hosts are shut down, boot them now. Booting the hosts enables IBM AIX to recognize the drives.

If the initiator site hosts are not shut down, use the following commands to recognize the drives and mount the file systems:

```
cfgmgr -v
```

```
mount all
```

- e. **Microsoft Windows NT-X86:** Reboot the hosts at the initiator site and log in using an account that has administrative privileges. You should be able to see all of the units by choosing **My Computer**.

- f. **Microsoft Windows 2000:**

- 1) If you *have not* changed the UNIT_OFFSET of any host connections since the hosts have been booted, you do not need to reboot the initiator site hosts.

- a) On each host, log in using an account that has administrative privileges.

- b) Open **Computer Management** and click **Disk Management**.

- c) After **Disk Management** has initialized, go to the **Action** menu and click **Rescan Disks**. All of the failed over units should appear in the right-hand pane. If Secure Path is not installed correctly, you will see each unit twice.

2) If you *have* changed the UNIT_OFFSET of any host connections, you must reboot that host. After the server has rebooted, log in using an account that has administrative privileges. You will see all of the units in **Computer Management > Disk Management**. If Secure Path is not installed correctly, you will see each drive twice.

- g. **Novell NetWare:** If the initiator site hosts are shut down, boot them now. Booting the hosts allows Novell NetWare to recognize the drives.

If the initiator site hosts are already up and running, or if they do not recognize the drives, issue the following command from the console before mounting the volumes:

```
SCAN FOR NEW DEVICES
```

Alternatively, you can use the `NWCONFIG` utility to issue this same command.

- h. **SUN Solaris:** Reboot the hosts using the command `reboot -- -r` at the initiator site and log in using an account that has administrative privileges. You should be able to see all of the units by using the `format` command.

If Secure Path was not configured for these units, you will not see the drives. You will need to edit the WWLIDs in the file `/kernel/drv/ldLite.conf`. To find the new WWLIDs of the units, use the `SHOW Unitname` command on the controller. You may also need to adjust the files `/kernel/drv/mda.conf` and `/kernel/drv/sd.conf` to accommodate the extras LUNs. When you have edited `ldLite.conf`, `mda.conf`, and `sd.conf`, reboot the host using the `reboot -- -r` command. You should now be able to see the drives using the `format` command. Refer to the *Compaq SANworks Secure Path for Sun Solaris Installation and Reference Guide* for additional assistance.

This completes the short duration planned failover with fast failback.

Resumption of Replication After Short Planned Loss of Target Procedure

This chapter contains these procedures to resume replication after a short duration planned communication loss at the target:

- “Suspend Remote Copy Sets for Target Site Shutdown” on page 6–2
- “Target Site Shutdown” on page 6–6
- “Resume Remote Copy Sets When Target Site Is Back Up” on page 6–7

NOTE: In this chapter, *initiator* site procedure steps are identified by an arrow symbol ► in the margin. *Target* site procedure steps are identified by a target symbol ② in the margin.

NOTE: Some example displays illustrate confirmation messages with the event log symbol (%EVL) and an instance code. Compare the instance code in the example with the instance code you receive. If the numbers are the same, you have performed the previous command correctly and have achieved the desired results. Note that you will be able to see these screens only if you are working from the controller to which the LUNs are online. Refer to the Troubleshooting chapter for more information on instance codes and their meanings.

Example displays may also contain bold text to identify information that is the most pertinent in the example. In many cases, items shown in bold text will help you verify the results of a previous command.

Procedure for Planned Loss of Target During Short Maintenance Period

In this situation you will be bringing the target site down for planned maintenance. The remote copy sets are in failsafe mode. The duration of the outage at the target is relatively short (up to several hours). You will not be performing failover or failback, but you will resume replication after the target site is operational and back online.

Use this procedure when the error mode of the remote copy set is set for failsafe and the target site will be temporarily shut down. Setting the error mode of the remote copy set to normal allows host I/O to continue while the target site is offline. Enabling write logging prevents the need for a full copy as long as the log unit does not have enough time to fill up.

Suspend Remote Copy Sets for Target Site Shutdown

This procedure ceases write operations to the target.

- ▶ 1. Verify that the remote copy sets have error modes set to failsafe with the following CLI command:

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to that in Example Display 1.

Example Display 1

```
BuildngATop> SHOW REMOTE_COPY_SETS FULL
Name                                     Uses                               Used by
-----
RCS1          remote copy                       D1                               AS_D1
Reported LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003E
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = FAILSAFE
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGA\D1) state:
  ONLINE to this controller
  Not reserved
Target state:
  BUILDNGB\D1      is NORMAL
```

- ▶ 2. Set the error mode of all remote copy set to normal mode with the following CLI command:

```
SET RemoteCopySetName ERROR_MODE = NORMAL
```

Example: set rcs1 error_mode = normal

Repeat this step for all remote copy sets.

- ▶ 3. Create a mirrorset for the log disk by issuing the following CLI command:

```
ADD MIRRORSET MirrorsetName DiskName1 DiskName2
```

Example: add mirr mir_d1log disk50100 disk60100

NOTE: To minimize the number of devices used for logging, you can create and use one-member mirrorsets. Because the data will be written to one disk, the logged data will not be protected. However, all of this data is also written to the initiator unit. In the case of a log disk failure, you would incur a full normalization, rather than a mini-merge, when access to the target is re-established.

The command to create a one-member mirrorset is the same as above, except only one disk is listed.

Example: add mirr mir_d1log disk50100.

IMPORTANT: If you will be using scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention (remote copy sets, stripesets, mirrorsets, RAIDsets, association sets, and connections)—use underscores instead. Dashes are not allowed by the Perl scripting language.

- ▶ 4. Initialize the mirrorset with the following CLI command:

```
INITIALIZE ContainerName
```

Example: initialize mir_d1log

- ▶ 5. Verify that you have created a mirrorset by issuing the following CLI command:

```
SHOW MIRRORSET
```

You will see a display similar to that in Example Display 2.

Example Display 2

Name	Storageset	Uses	Used by
MIR_D1LOG	mirrorset	DISK50100 DISK60100	

- ▶ 6. Present the log unit to the controller with the following CLI command:

```
ADD UNIT UnitName ContainerName
```

Example: add unit d10 mir_d1log

- ▶ 7. Verify that the controller recognizes the log unit by issuing the following CLI command:

```
SHOW UNITS
```

You will see a display similar to that in Example Display 3.

Example Display 3

LUN	Uses	Used by
D10	MIR_D1LOG	

- ▶ 8. Disable node access to the log unit with the following CLI command:

```
SET UnitNumber DISABLE_ACCESS_PATH = ALL
```

Example: set d10 disable_access_path = all

- ▶ 9. Disable writeback cache with the following CLI command:

```
SET UnitNumber NOWRITEBACK_CACHE
```

Example: set d10 nowriteback_cache

- ▶ 10. Check to see that you have disabled access and writeback cache with the following command:

```
SHOW D10
```

You will see a display similar to that in Example Display 4.

Example Display 4

LUN	Uses	Used by
D10	MIR_D1LOG	
LUN ID:	6000-1FE1-0001-3B10-0009-9130-8044-0066	
IDENTIFIER =	10	
Switches:		
RUN	NOWRITE_PROTECT	READ_CACHE
READAHEAD_CACHE	NOWRITEBACK_CACHE	
MAXIMUM_CACHED_TRANSFER_SIZE =	32	
Access:		
None		
State:		
ONLINE to this controller		
Not reserved		
PREFERRED_PATH =	THIS_CONTROLLER	
Size:	35556389 blocks	
Geometry (C/H/S):	(7000 / 20 / 254)	

- ▶ 11. Create an association set with the following CLI command:

```
ADD ASSOCIATIONS AssociationSetName RemoteCopySetName
```

Example: `add associations as_d1 rcs1`

IMPORTANT: If you will be using scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention (remote copy sets, stripesets, mirrorsets, RAIDsets, association sets, and connections)—use underscores instead. Dashes are not allowed by the Perl scripting language.

NOTE: You can add additional members to the association set by issuing the following CLI command:

```
SET AssociationSetName ADD = RemoteCopySetName
```

- ▶ 12. Assign the log unit to the association set with the following CLI command:

```
SET AssociationSetName LOG_UNIT = D10
```

Example: `set as_d1 log_unit = d10`

- ▶ 13. Check to see the switch status of the association set by issuing the following CLI command:

```
SHOW AssociationSetName
```

Example: `show as_d1`

You will see a display similar to that in Example Display 5.

Example Display 5

```

Name                Association                Uses                Used by
-----
D1                  association                RC_D1                AS_
Switches:
  NOFAIL_ALL
  NOORDER_ALL
LOG_UNIT = D10 (No data logged)

```

- ▶ 14. Use the following CLI command to verify that the remote copy set's error mode is set to normal, that it uses an association set, and to obtain the TargetName\UnitName from the target state:

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to that in Example Display 6.

Example Display 6

```

BuildngATop> SHOW REMOTE_COPY_SETS FULL
Name                Uses                Used by
-----
RCS1                remote copy        D1                AS_D1
Reported LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003E
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE = NORMAL
  FAILOVER_MODE = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGA\D1) state:
  ONLINE to this controller
  Not reserved
Target state:
  BUILDNGB\D1 is NORMAL

```

- ▶ 15. Suspend write operations to the target site with the following CLI command:

```
SET RemoteCopySetName SUSPEND = TargetName\UnitName
```

Example: set rcs1 suspend = buildngb\d1

Repeat this step for all remote copy sets.

You will see a confirmation message, as shown in Example Display 7.

Example Display 7

```

%EVL--BuildngATop> --07-JUN-2001 11:51:01-- Instance Code: 0E210064
Template: 144.(90)
.
.
.

```

Instance Code: 0E210064

- ▶ 16. Use the following CLI command to verify that the remote copy sets are suspended and that the log unit is available:

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to that in Example Display 8.

Example Display 8

```
BuildngATop> SHOW REMOTE_COPY_SETS FULL
Name                               Uses                               Used by
-----
RCS1      remote copy                       D1                               AS_D1
Reported LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003E
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGA\D1) state:
  ONLINE to this controller
  Not reserved
Target state:
  BUILDNGB\D1      is SUSPENDED      LOG_UNIT 96% available
```

Target Site Shutdown

1. If necessary for the type of maintenance being performed, shut down the controllers at the target site. The procedure for site shutdown is contained in Appendix B.
2. Continue the resumption of operations with the following procedure for resuming remote copy sets.
3. Power up the target site if it was powered off. The procedure for site powerup is contained in Appendix B.

Resume Remote Copy Sets When Target Site Is Back Up

- ▶ 1. Once the target site is back up, look for a confirmation message, as shown in Example Display 9.

Example Display 9

```
BuildngATop>
%EVL--BuildngATop> --07-JUN-2001 12:08:20-- Instance Code: 0E120064
  Template: 144.(90)
  .
  .
Instance Code: 0E120064
```

- ▶ 2. Resume write operations to the target site with this CLI command:

```
SET RemoteCopySetName RESUME = TargetName\UnitName
```

```
Example: set rcs1 resume = buildngb\d1
```

Repeat this step for all remote copy sets.

- ▶ 3. After you have completed this command, you will see a confirmation message, as shown in Example Display 10.

Example Display 10

```
%EVL--BuildngATop> --07-JUN-2001 12:09:41-- Instance Code: 0E220064
  Template: 144.(90)
  .
  .
Instance Code: 0E220064
```

- ▶ 4. Use the following CLI command to verify that the remote copy sets are merging:

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to that in Example Display 11.

Example Display 11

```
BuildngATop> SHOW REMOTE_COPY_SETS FULL
Name                               Uses                               Used by
-----
RCS1      remote copy                    D1                               AS_D1
Reported LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003E
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGA\D1) state:
  ONLINE to this controller
  Not reserved
Target state:
  BUILDNGB\D1      is MERGING                               1% complete
```

- ▶ 5. Once the merge has completed, you will see a confirmation message, as shown in Example Display 12.

Example Display 12

```
BuildngATop>
%EVL--BuildngATop> --07-JUN-2001 12:11:49-- Instance Code: 0E110064
Template: 144.(90)
.
.
.
Instance Code: 0E110064
```

- ▶ 6. Use the following CLI command to verify that the target state of the remote copy set is set to **NORMAL**:

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to that in Example Display 13.

Example Display 13

```
BuildngATop> SHOW REMOTE_COPY_SETS FULL
Name                               Uses                               Used by
-----
RCS1      remote copy                    D1                               AS_D1
Reported LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003E
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGA\D1) state:
  ONLINE to this controller
  Not reserved
Target state:
  BUILDNGB\D1      is NORMAL
```

IMPORTANT: Wait for normalization on all remote copy sets to complete before proceeding.

- ▶ 7. Turn off write history logging with the following CLI command:

```
SET AssociationSetName NOLOG_UNIT
```

Example: set as_d1 nolog_unit

- ▶ 8. Use the following CLI command to verify that the association sets have no log unit:

```
SHOW ASSOCIATION FULL
```

You will see a display similar to that in Example Display 14.

Example Display 14

```
BuildngATop> SHOW ASSOCIATION FULL
Name                               Association                          Uses                               Used by
-----
AS_D1      association                          RCS1
Switches:
  NOFAIL_ALL
  NOORDER_ALL
  NOLOG_UNIT
```

- ▶ 9. If you have configured an association set, remove it now with the following CLI command:

```
DELETE AssociationSetName
```

Example: delete as_d1

- ▶ 10. Set the error mode of the remote copy set back to failsafe with the following CLI command:

```
SET RemoteCopySetName ERROR_MODE = FAILSAFE
```

Example: set rcs1 error_mode = failsafe

Repeat this step for all remote copy sets.

- ▶ 11. Use the following CLI command to verify that the error mode of the remote copy set is set back to failsafe:

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to that in Example Display 15.

Example Display 15

```
BuildngATop> SHOW REMOTE_COPY_SETS FULL
Name                               Uses                               Used by
-----
RCS1      remote copy                       D1                               AS_D1
Reported LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003E
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE    = FAILSAFE
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGA\D1) state:
  ONLINE to this controller
  Not reserved
Target state:
  BUILDNGB\D1      is NORMAL
```

This completes the procedure for resumption of operations after a planned loss of target for a short maintenance period.

Extended Planned Site Failover With Full Failback Procedure

In this situation you will be performing planned maintenance at the initiator site. The maintenance will not be completed within a relatively short period of time. You will perform a failover to the target site. Because of the longer duration of the planned outage, the write history log will not be able to accommodate the accumulated reads and writes. Because the write history log cannot capture all host I/O, when the initiator is operational and back online, you will perform a full failback to the initiator.

This chapter contains the following procedures to ensure that failover and subsequent failback performed for initiator site maintenance function properly:

- “Planned Site Failover” on page 7–2
- “Maintenance Completion” on page 7–16
- “Maintenance Failback” on page 7–20

NOTE: In this chapter, *initiator* site procedure steps are identified by an arrow symbol ► in the margin. *Target* site procedure steps are identified by a target symbol ☉ in the margin.

NOTE: Some example displays illustrate confirmation messages with the event log symbol (%EVL) and an instance code. Compare the instance code in the example with the instance code you receive. If the numbers are the same, you have performed the previous command correctly and have achieved the desired results. Note that you will be able to see these screens only if you are working from the controller to which the LUNs are online. Refer to the Troubleshooting chapter for more information on instance codes and their meanings.

Example displays may also contain bold text to identify information that is the most pertinent in the example. In many cases, items shown in bold text will help you verify the results of a previous command.

Planned Site Failover

Use Planned Site Failover when the initiator site will be undergoing maintenance. Planned Site Failover consists of the following procedures:

- Initiator Site Preparation Procedure
- Target Site Failover Procedure
- Target Host Setup Procedure

Initiator Site Preparation Procedure

- ▶ 1. Before performing the failover procedure, locate your record of SHOW command output that details the current initiator configuration. Verify that your target controller configuration is the same as your initiator controller configuration. Compare the status of the controllers, association sets, remote copy sets, units, and connections. Appendix A contains the full procedure.
- ▶ 2. Verify that all remote copy sets are in normal state. Issue the following CLI command:

```
SHOW REMOTE_COPY_SETS FULL
```

The output shows the status of remote copy sets.

You will see a display similar to that in Example Display 1.

Example Display 1

```
BuildngATop> show remote_copy_sets full
Name                               Uses                               Used by
-----
RCS1      remote copy                       D1                               AS_D1
Reported LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0134
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGA\D1) state:
  ONLINE to this controller
  Not reserved
Target state:
  BUILDNGB\D1      is NORMAL
RCS2      remote copy                       D2
Reported LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0135
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
```

```
Initiator (BUILDNGA\D2) state:  
  ONLINE to this controller  
  Not reserved  
Target state:  
  BUILDNGB\D2          is NORMAL
```

- ▶ 3. Follow the steps listed below for each operating system in your heterogeneous configuration:
- Compaq OpenVMS:** If the operating system is up and running, and is being used exclusively for DRM operations, shut down the operating system and power off the hosts. If the operating system is being used for other applications, remove all I/O to the remote copy set LUNs that will be failed over, then dismount the volumes associated with these LUNs.
 - Compaq Tru64 UNIX:** If the operating system is up and running and is being used exclusively for DRM operations, shut down the operating system and power off the hosts. If the operating system is being used for other applications, remove all I/O and unmount all file system LUNs that have remote copy sets that will be failed over.
 - HP-UX:** If the operating system is up and running, remove all I/O to the remote copy set LUNs that will be failed over, then unmount the file systems associated with these LUNs.
 - IBM AIX:** If the operating system is up and running, remove all I/O to the remote copy set LUNs that will be failed over, then unmount the file systems associated with these LUNs.
 - Microsoft Windows NT-X86:** If the operating system is up and running, shut it down and power off the hosts.
 - Microsoft Windows 2000:** If the operating system is up and running, shut it down and power off the hosts.
 - Novell NetWare:** If the operating system is up and running, remove all I/O to the remote copy set LUNs that will be failed over, then dismount the volumes associated with these LUNs.

If you are using NetWare Cluster Services (NWCS), you must enter the `cluster down` command. You must also enter the `uldncs` (unload NetWare Cluster Services) command for all cluster nodes.



CAUTION: Failure to enter these two commands will cause all cluster nodes to abend.

- h. **SUN Solaris:** If the operating system is up and running and is being used exclusively for DRM operations, shut down the operating system and power off the hosts. If the operating system is being used for other applications, remove all I/O and unmount all volumes that have remote copy sets that will be failed over.

- ▶ 4. If your remote copy sets are set for asynchronous operation mode, switch to synchronous mode using the following CLI command:

```
SET RemoteCopySetName OPERATION_MODE = SYNCHRONOUS
```

Example: set rcs1 operation_mode = synchronous

Repeat this step for all applicable remote copy sets.

- ▶ 5. Turn off write history logging, if enabled, with the following CLI command:

```
SET AssociationSetName NOLOG_UNIT
```

Example: set as_d1 nolog_unit

Repeat this step for each applicable association set.

- ▶ 6. If you have association sets, delete them with the following CLI command:

```
DELETE AssociationSetName
```

Example: delete as_d1

Repeat this step for each applicable association set.

- ▶ 7. Disable host access to the remote copy set units with the following CLI command:

NOTE: Do not disable access to the target connection.

```
SET UnitName DISABLE = InitiatorHostConnectionNameX,  
InitiatorHostConnectionNameY
```

Example: set d1 disable = hosta1,hosta2

Repeat this step for all remote copy set units.

- ▶ 8. Each remote copy set unit should have four connections enabled to TargetRemoteCopyNameA, TargetRemoteCopyNameB, TargetRemoteCopyNameC, and TargetRemoteCopyNameD.

- a. To see the connections, enter the following CLI command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 2.

Example Display 2

```

BuildngATop> show units full
      LUN                               Uses                               Used by
-----
D1
LUN ID:      6000-1FE1-0000-01F0-0009-8490-6303-0134
NOIDENTIFIER
Switches:
  RUN                               NOWRITE_PROTECT           READ_CACHE
  READAHEAD_CACHE                   WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  BUILDNGBA, BUILDNGBB, BUILDNGBC, BUILDNGBD
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = THIS_CONTROLLER
Size:      17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )

D2
LUN ID:      6000-1FE1-0000-01F0-0009-8490-6303-0135
NOIDENTIFIER
Switches:
  RUN                               NOWRITE_PROTECT           READ_CACHE
  READAHEAD_CACHE                   WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  BUILDNGBA, BUILDNGBB, BUILDNGBC, BUILDNGBD
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = OTHER_CONTROLLER
Size:      17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )

```

- b. If access to the target site controllers is not currently enabled, enable access by issuing the following command for each applicable remote copy set unit:

```

SET UnitName ENABLE = TargetRemoteCopyNameA,
TargetRemoteCopyNameB, TargetRemoteCopyNameC,
TargetRemoteCopyNameD

```

Example: set d1 enable = buildngbA,buildngbB,buildngbC, buildngbD

- ▶ 9. Set the maximum cached transfer size to 128 with the following CLI command:

```

SET UnitName MAXIMUM_CACHED_TRANSFER_SIZE = 128

```

Example: set d1 maximum_cached_transfer_size = 128

Repeat this step for all remote copy set units.

NOTE: This command sets both the read and write maximum cached transfer size.

- ▶ 10. If you need to shut down the initiator controllers, proceed with the following CLI commands (in this order):


```
SHUTDOWN OTHER_CONTROLLER
SHUTDOWN THIS_CONTROLLER
```
- ▶ 11. After the preceding command has completed and both controllers have shut down successfully, power off the controller rack. See Appendix B for the power down procedure.

If the initiator site will be powered down for a long period of time, you may need to disable cache batteries.
- ▶ 12. Continue the Planned Failover at the target site with the Target Site Failover Procedure.

Target Site Failover Procedure

- ◎ 1. At the target site, the remote copy set units must be preferred to one controller or the other.
 - a. Use the following CLI command to check for the preferred path:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 3.

Example Display 3

```
BuildngBTop> show units full
LUN
-----
D1
LUN ID:          6000-1FE1-0000-4250-0009-9411-5654-003E
NOIDENTIFIER
Switches:
  RUN              NOWRITE_PROTECT      READ_CACHE
  READAHEAD_CACHE  WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 128
  MAX_WRITE_CACHED_TRANSFER_SIZE = 128
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = THIS_CONTROLLER
  Target NORMAL
Size:          17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
```

```

D2                                DISK20000                                BUILDNGA\RCS2
LUN ID:                          6000-1FE1-0000-4250-0009-9411-5654-003F
NOIDENTIFIER
Switches:
  RUN                             NOWRITE_PROTECT                                READ_CACHE
  READAHEAD_CACHE                 WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 128
  MAX_WRITE_CACHED_TRANSFER_SIZE = 128
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = OTHER_CONTROLLER
  Target NORMAL
Size:                             17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )

```

- b. If remote copy set units are not currently preferred, use the following CLI command:

```

SET UnitName PREFERRED_PATH = THIS_CONTROLLER
Example: set d1 preferred_path = this_controller

```

or

```

SET UnitName PREFERRED_PATH = OTHER_CONTROLLER
Example: set d2 preferred_path = other_controller

```

Repeat this step for each remote copy set unit that needs to be preferred.

2. Disconnect controller access with the following CLI commands:

```

SET THIS_CONTROLLER PORT_2_TOPOLOGY = OFFLINE
SET OTHER_CONTROLLER PORT_2_TOPOLOGY = OFFLINE

```

3. Verify controller access disconnection with the following CLI commands:

```

SHOW THIS_CONTROLLER
SHOW OTHER_CONTROLLER

```

You will see a display similar to that in Example Display 4.

Example Display 4

```

BuildngBTop> show this_controller
Controller:
  HSG80 ZG84906303 Software V86-1P, Hardware E03
  NODE_ID          = 5000-1FE1-0000-01F0
  ALLOCATION_CLASS  = 0
  SCSI_VERSION     = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG84906237
  In dual-redundant configuration
  Device Port SCSI address 7
  Time: 10-MAY-2001 17:55:29

```

```

        Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-01F3
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address          = 220213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-01F4
  PORT_2_TOPOLOGY = OFFLINE (offline)
  REMOTE_COPY = BUILDNGB
.
.
BuildngBTop> show other_controller
Controller:
  HSG80 ZG84906237 Software V86-1P, Hardware E03
  NODE_ID          = 5000-1FE1-0000-01F0
  ALLOCATION_CLASS = 0
  SCSI_VERSION     = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG84906303
  In dual-redundant configuration
  Device Port SCSI address 6
  Time: 10-MAY-2001 17:55:39
  Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-01F1
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address          = 250213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-01F2
  PORT_2_TOPOLOGY = OFFLINE (offline)
  REMOTE_COPY = BUILDNGA
.
.

```

- ④ 4. Move the initiator role to the target with the following CLI command:

```
SITE_FAILOVER InitiatorRemoteCopyName\RemoteCopySetName
```

```
Example: site_failover buildngA\rsc1
```

NOTE: The *InitiatorRemoteCopyName* is the remote copy name of the original initiator.

You will see a confirmation message, as shown in Example Display 5.

Example Display 5

```

BuildngBTop> site_failover buildngA\rsc1

%EVL--BuildngBTop> --10-MAY-2001 15:47:39-- Instance Code: 0E010064
  Template: 144.(90)
.
.
Instance Code: 0E010064

```

Repeat this step for each remote copy set.

- ⑤ 5. Remove the targets with the following CLI command:

```
SET RemoteCopySetName REMOVE = InitiatorRemoteCopyName\UnitNumber
```

```
Example: set rcs1 remove = buildngA\d1
```

You will see a confirmation message, as shown in Example Display 6.

Example Display 6

```
BuildngBTop> set rcs1 remove=buildngA\d1
%EVL--BuildngBTop> --10-MAY-2001 16:49:55-- Instance Code: 0E078A01
Template: 144.(90)
.
.
Instance Code: 0E078A01
```

Repeat this step for each remote copy set.

- ⑥ 6. To restore the connections to the target site, issue the following CLI commands:

```
SET THIS_CONTROLLER PORT_2_TOPOLOGY = FABRIC
```

```
SET OTHER_CONTROLLER PORT_2_TOPOLOGY = FABRIC
```

- ⑦ 7. Verify connection restoration with the following CLI commands:

```
SHOW THIS_CONTROLLER
```

```
SHOW OTHER_CONTROLLER
```

You will see a display similar to that in Example Display 7.

Example Display 7

```
BuildngBTop> show this_controller
Controller:
  HSG80 ZG94115654 Software V86-1P, Hardware E10
  NODE_ID = 5000-1FE1-0000-4250
  ALLOCATION_CLASS = 0
  SCSI_VERSION = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG94319198
  In dual-redundant configuration
  Device Port SCSI address 7
  Time: 10-MAY-2001 17:34:11
  Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-4253
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address = 260213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-4254
  PORT_2_TOPOLOGY = FABRIC (fabric up)
  Address = 260413
  REMOTE_COPY = BUILDNGB
.
.
```

```
.
BuildngBTop> show other_controller
Controller:
  HSG80 ZG94319198 Software V86-1P, Hardware E10
  NODE_ID           = 5000-1FE1-0000-4250
  ALLOCATION_CLASS   = 0
  SCSI_VERSION      = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG94115654
  In dual-redundant configuration
  Device Port SCSI address 6
  Time: 10-MAY-2001 17:34:20
  Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-4251
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address          = 200213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-4252
  PORT_2_TOPOLOGY = FABRIC (fabric up)
  Address          = 200413
  REMOTE_COPY     = BUILDNGB
.
.
.
```

8. Obtain your record of `SHOW` command output that details the original initiator configuration. Using the output as a reference, create association sets to duplicate those that were on the initiator. For information on how to create association sets, see Appendix C.

IMPORTANT: If you will be using scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention (remote copy sets, stripesets, mirrorsets, RAIDsets, association sets, and connections)—use underscores instead. Dashes are not allowed by the Perl scripting language.

Repeat this step for each applicable association set. You can set up write history logging after you add targets back to the configuration, later in this chapter.

9. Continue the Planned Failover at the target site with the Target Host Setup Procedure.

Target Host Setup Procedure

1. If you wish, you can enhance host I/O performance by resetting the maximum cached transfer size to the value used on the initiator. Obtain your record of `SHOW` command output that details the original initiator configuration. Using the output as a reference, set the maximum cached transfer size to the original initiator value using the following CLI command:

```
SET UnitName MAXIMUM_CACHED_TRANSFER_SIZE = InitiatorValue
```

```
Example: set d1 maximum_cached_transfer_size = 32
```

Repeat this step for each remote copy set unit.

NOTE: The default maximum cached transfer size is 32.

- 2. Enable host access to all remote copy set units at the target site with the following CLI command:

```
SET UnitName ENABLE = TargetHostConnectionNamex,
TargetHostConnectionNamey
```

Example: set d1 enable = hostb1,hostb2

You will see a display similar to that in Example Display 8.

Example Display 8

```
BuildngBTop> set d1 enable=hostb1,hostb2
Warning 1000: Other host(s) in addition to the one(s) specified can still
              access this unit. If you wish to enable ONLY the host(s)
              specified, disable all access paths (DISABLE_ACCESS=ALL), then
              again enable the ones specified
```

Repeat this step for each remote copy set unit.

- 3. If you do not recall a target host connection name, use the following command:

```
SHOW CONNECTIONS
```

You will see a display similar to that in Example Display 9.

Example Display 9

```
BuildngBTop> show connections
Connection
Name      Operating system      Controller  Port  Address  Status  Unit
Offset
BUILDNGAA  PPRC_TARGET          THIS        2     220413  offline 0
HOST_ID=5000-1FE1-0000-01F0  ADAPTER_ID=5000-1FE1-0000-01F4
BUILDNGAB  PPRC_TARGET          OTHER       2     220413  offline 0
HOST_ID=5000-1FE1-0000-01F0  ADAPTER_ID=5000-1FE1-0000-01F2
BUILDNGAC  PPRC_INITIATOR       THIS        2     220413  OL this  0
HOST_ID=5000-1FE1-0000-01F0  ADAPTER_ID=5000-1FE1-0000-01F4
BUILDNGAD  PPRC_INITIATOR       OTHER       2     250413  OL other 0
HOST_ID=5000-1FE1-0000-01F0  ADAPTER_ID=5000-1FE1-0000-01F2
HOSTA1     WINNT                 THIS        1     260013  OL this  0
HOST_ID=1000-0000-C920-A7B9  ADAPTER_ID=1000-0000-C920-A7B9
HOSTA2     WINNT                 OTHER       1     200013  OL other 0
HOST_ID=1000-0000-C921-3F4E  ADAPTER_ID=1000-0000-C921-3F4E
HOSTB1    WINNT                 THIS        1     220013  OL this  0
HOST_ID=1000-0000-C921-3E98  ADAPTER_ID=1000-0000-C921-3E98
HOSTB2    WINNT                 OTHER       1     250013  OL other  0
```

HOST_ID=1000-0000-C921-3EFC

ADAPTER_ID=1000-0000-C921-3EFC

- ④ 4. Verify access to the target site hosts with the following CLI command:

SHOW UNITS FULL

You will see a display similar to that in Example Display 10.

Example Display 10

BuildngBTop> show units full

LUN	Uses	Used by
D1	DISK10000	BUILDNGB\RCS1
LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003E NOIDENTIFIER Switches: RUN NOWRITE_PROTECT READ_CACHE READAHEAD_CACHE WRITEBACK_CACHE MAX_READ_CACHED_TRANSFER_SIZE = 32 MAX_WRITE_CACHED_TRANSFER_SIZE = 32 Access: BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD, HOSTB1, HOSTB2 State: ONLINE to this controller Not reserved PREFERRED_PATH = THIS_CONTROLLER Size: 17769177 blocks Geometry (C/H/S): (5258 / 20 / 169)		
D2	DISK20000	BUILDNGB\RCS2
LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003F NOIDENTIFIER Switches: RUN NOWRITE_PROTECT READ_CACHE READAHEAD_CACHE WRITEBACK_CACHE MAX_READ_CACHED_TRANSFER_SIZE = 32 MAX_WRITE_CACHED_TRANSFER_SIZE = 32 Access: BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD, HOSTB1, HOSTB2 State: ONLINE to this controller Not reserved PREFERRED_PATH = OTHER_CONTROLLER Size: 17769177 blocks Geometry (C/H/S): (5258 / 20 / 169)		

In the Access field of the display, all units that are used by remote copy sets will show that both the target host and the initiator controller connections are enabled.

- ④ 5. Allow hosts to recognize new units. Follow the steps listed below for each operating system in your heterogeneous configuration:
 - a. **Compaq OpenVMS:** If the target site hosts are shut down, boot them now. Booting the hosts enables OpenVMS to recognize the drives.

If the target site hosts are not shut down, use the following command from a privileged account to enable OpenVMS to recognize the drives:

```
MCR SYSMAN IO AUTOCONFIGURE/LOG
```

- b. **Compaq Tru64 UNIX:** If the target site hosts are shut down, boot them now. Booting the hosts enables Tru64 UNIX to recognize the drives.

If the target site hosts are not shut down, use the following command to recognize the drives:

```
hwmgr - scan scsi
```

This might take a while for large configurations. If this is the case, scan only those SCSI buses that have new units added. Scan only one bus at a time. Use the following command:

```
hwmgr -scan scsi -bus x
```

where x is the SCSI bus number.

- c. **HP-UX:**

- 1) If the target site hosts are shut down, boot them now. Booting the hosts enables HP-UX to recognize the drives.

If the target site hosts are not shut down, use the following command to enable HP-UX to recognize the drives and verify that they are present. This command will display only the previously configured failed-over LUNs:

```
ioscan -fnCdisk
```

- 2) Continue with the following commands to access file systems on new failed-over LUNs. If you have no new failed-over LUNs, skip these substeps and go directly to the next step to mount the LUNs:

- a. `/opt/CPQswsp/spmgr display -u`

- b. `/opt/CPQswsp/spmgr add WWN`

Repeat this command for each un-attached WWN that was displayed.

- c. `ioscan -fnCdisk`

If the device special files were not displayed, run `insf -e`, then run `ioscan -fnCdisk` again.

- d. `vgimport VolumeGroupName DeviceSpecialFile`

Repeat this command for each new failed-over LUN.

3) Use the following command to mount the LUNs:

```
mount -a
```

NOTE: *VolumeGroupName* is the name of the volume group you originally created at the initiator site. The *DeviceSpecialFiles* are from the *ioscan* in the form of */dev/dsk/c_t_d_*.

For consistency, configure the same *DeviceSpecialFiles* with the same volume groups, logical volumes, and file systems for the failed-over LUNs at the target site with the same LUNs at the initiator site.

- d. **IBM AIX:** If the target site hosts are shut down, boot them now. Booting the hosts enables IBM AIX to recognize the drives.

If the target site hosts are not shut down, use the following commands to enable AIX to recognize the drives and verify that they are present:

```
cfgmgr -v  
lsdev -Cc disk
```

Use the following commands to access file systems on the failed-over LUNs:

```
importvg -y volumegroupname hdiskx  
mount all
```

NOTE: *volumegroupname* is the name of the volume group you originally created at the initiator site, and *x* is the number of the *hdisk* assigned to the failed-over LUN. If the *-y volumegroupname* parameter is omitted, AIX will create a default volume group name for you, for example, *vg00*.

- e. **Microsoft Windows NT-X86:** Reboot the hosts at the target site and log in using an account that has administrative privileges. You should be able to see all of the units by choosing **My Computer**.
- f. **Microsoft Windows 2000:**
- 1) If you *have not* changed the `UNIT_OFFSET` of any host connections since the hosts have been booted, you do not need to reboot the initiator site hosts.
 - a) On each host, log in using an account that has administrative privileges.
 - b) Open **Computer Management** and click **Disk Management**.
 - c) After **Disk Management** has initialized, go to the **Action** menu and click **Rescan Disks**. All of the failed over units should appear in the right-hand pane. If Secure Path is not installed correctly, you will see each unit twice.

2) If you *have* changed the UNIT_OFFSET of any host connections, you must reboot that host. After the server has rebooted, log in using an account that has administrative privileges. You will see all of the units in **Computer Management > Disk Management**. If Secure Path is not installed correctly, you will see each drive twice.

- g. **Novell NetWare:** If the target site hosts are shut down, boot them now. If you are using traditional NetWare volumes, booting the hosts allows Novell NetWare to recognize the drives and automatically mount the volumes. If you are using NSS logical volumes, booting the hosts will recognize the NSS pools and activate them. However, you must manually mount each individual NSS volume by typing `MOUNT VolumeName` at the NetWare console.

If the target site hosts are already up and running, or if they do not recognize the drives, issue the following command from the console before mounting the volumes:

```
SCAN FOR NEW DEVICES
```

Alternatively, you can use the `NWCONFIG` utility to issue this same command.

Next, mount the volumes with these commands:

```
MOUNT ALL (for traditional NetWare volumes)
```

```
MOUNT VolumeName (for NSS logical volumes).
```

- h. **SUN Solaris:** Reboot the hosts using the command `reboot -- -r` at the target site and log in using an account that has administrative privileges. You should be able to see all of the units by using the `format` command.

If Secure Path was not configured for these units, you will not see the drives. You will need to edit the WWLIDs in the file `/kernel/drv/ldLite.conf`. To find the new WWLIDs of the units, use the `SHOW Unitname` command on the controller. You may also need to adjust the files `/kernel/drv/mda.conf` and `/kernel/drv/sd.conf` to accommodate the extras LUNs. When you have edited `ldLite.conf`, `mda.conf`, and `sd.conf`, reboot the host using the `reboot -- -r` command. You should now be able to see the drives using the `format` command. Refer to the *Compaq SANworks Secure Path for Sun Solaris Installation and Reference Guide* for additional assistance.

This completes Planned Failover. Stop at this point.

IMPORTANT: Proceed with the following Maintenance Completion only after the maintenance work on the initiator controller is completed and the targets are ready to be added back in.

Maintenance Completion

Compare the status of the controllers, association sets, remote copy sets, units, and connections at the target site with those at the initiator site. A full procedure is detailed in Appendix A. Make sure any status change is reflected on the target. To compare status, bring up a terminal emulator session and enter a `SHOW THIS` command.

Maintenance Completion consists of the following procedures:

- Initiator Site Preparation Procedure
- Target Site Copy Data Procedure

Initiator Site Preparation Procedure

- ▶ 1. Power up the controllers, if necessary. See Appendix B for the powerup procedure.
- ▶ 2. Check all units for lost data with the following CLI command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 11.

Example Display 11

```
BuildngATop> show units full
-----
LUN                               Uses                               Used by
-----
D1                                DISK10000                          Buildnga\RCS1
LUN ID:                           6000-1FE1-0007-9DD0-0009-0510-3907-000C
NOIDENTIFIER
Switches:
  RUN                               NOWRITE_PROTECT                     READ_CACHE
  READAHEAD_CACHE                   WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 128
  MAX_WRITE_CACHED_TRANSFER_SIZE = 128
Access:
  BUILDNGBA, BUILDNGBB, BUILDNGBC, BUILDNGBD
State:
  INOOPERATIVE
  Unit has lost data
  UNKNOWN - Unit is no longer an initiator
  PREFERRED_PATH = THIS_CONTROLLER
  WRITE_PROTECT - DATA SAFETY
Size:                                NOT YET KNOWN
```

Geometry (C/H/S): NOT YET KNOWN

- a. If there are units with lost data, clear the data for each applicable unit, with the following CLI command:

```
CLEAR_ERRORS UnitName LOST_DATA
```

Example: clear_errors d1 lost_data

- b. Verify that all the lost data has been cleared with the following CLI command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 12. If the lost data has been cleared, the display will indicate that the unit is ONLINE.

Example Display 12

```
BuildngATop> show units full
-----
LUN                               Uses                               Used by
-----
D1                                DISK10000                          BUILDNGA\RCS1
LUN ID:                           6000-1FE1-0000-01F0-0009-8490-6303-0134
NOIDENTIFIER
Switches:
  RUN                               NOWRITE_PROTECT                     READ_CACHE
  READAHEAD_CACHE                  WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFR_SIZE = 128
  MAX_WRITE_CACHED_TRANSFER_SIZE = 128
Access:
  BUILDNGBA, BUILDNGBB, BUILDNGBC, BUILDNGBD
State:
ONLINE to the other controller
  UNKNOWN - Unit is no longer an initiator
  PREFERRED_PATH = THIS_CONTROLLER
Size:                               17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
```

- ▶ 3. Delete all remote copy sets with following CLI command:

```
DELETE RemoteCopySetName
```

Example: delete rcs1

You will see a confirmation message, as shown in Example Display 13.

Example Display 13

```
BuildngATop> delete rcs1

%EVL--BuildngATop> --10-MAY-2001 18:01:12-- Instance Code: 0E020064
  Template: 144.(90)
  .
  .
Instance Code: 0E020064
```

Repeat this step for each remote copy set.

- ▶ 4. Continue with Maintenance Completion at the target site with the Target Site Copy Data Procedure.

Target Site Copy Data Procedure

This section describes how to copy the data from the target site to the initiator site. It starts the process, which is continued in the Maintenance Failback section.

- ⊙ 1. If you changed an asynchronous remote copy set to synchronous during failover, change it back to asynchronous mode by issuing the following CLI command:

```
SET RemoteCopySetName OPERATION_MODE = ASYNCHRONOUS
```

Example: `set rcs1 operation_mode = asynchronous`

Repeat this step for all applicable remote copy sets.

- ⊙ 2. Add back the target to the initiator unit's remote copy sets with the following CLI command:

```
SET RemoteCopySetName ADD = InitiatorRemoteCopyName\UnitName
```

Example: `set rcs1 add = buildngA\d1`

You will see a confirmation message, as shown in Example Display 14.

Example Display 14

```
BuildngBTop> set rcs1 add = BuildngA\d1
%EVL--BuildngBTop> --10-MAY-2001 17:37:27-- Instance Code: 0E050064
  Template: 144.(90)
  .
  .
  .
Instance Code: 0E050064
```

Repeat this step for all remote copy sets.

- ⊙ 3. Enter the following command to see the percentage of completion.

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to that in Example Display 15.

Example Display 15

```
BuildngBTop> show remote_copy_sets full
Name                               Uses           Used by
-----
RCS1      remote copy           D1             AS_D1
          Reported LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0134
```

```

Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGB\D1) state:
  ONLINE to the other controller
Target state:
  BUILDNGA\D1      is COPYING          94% complete

BuildngBTop> show remote_copy_sets full
Name                               Uses                               Used by
-----
RCS1      remote copy                D1                               AS_D1
Reported LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0134
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGB\D1) state:
  ONLINE to the other controller
Target state:
  BUILDNGA\D1      is NORMAL
  
```

When the units are all normalized, the Target state field of the display will show NORMAL.

IMPORTANT: Wait for normalization on all remote copy sets to complete before you proceed.

- ④ 4. If you plan to leave load running, you may now add write history logging to your association sets.

NOTE: For information on how to add write history logging to association sets, see Appendix C.

- ④ 5. If you plan to leave load running, and your application requires failsafe mode , set failsafe mode with the following CLI command:

```
SET RemoteCopySetName ERROR_MODE = FAILSAFE
```

Example: set rcs1 error_mode = failsafe

NOTE: Failsafe cannot be set if the remote copy set is in an association set that will be used for write history logging.

This completes Maintenance Completion. The next section describes how to perform Maintenance Failback.

Maintenance Failback

Maintenance Failback consists of the following procedures:

- Continuation of Target Site Copy Data Procedure
- Initiator Site Return Control Procedure
- Target Site Restore Procedure
- Initiator Site Restoration of Target Connections Procedure



CAUTION: The system must be in a failed over condition from the initiator site to the target site before beginning this procedure.

Continuation of Target Site Copy Data Procedure

This section continues the description that began in the Maintenance Completion section of how to copy the data from the target site to the initiator site.

1. Stop I/O from the target hosts to the remote copy set units.
2. Disable host access to all units used by remote copy sets at the target site, with the following CLI command:

```
SET UnitName DISABLE = TargetHostConnectionNamex,  
TargetHostConnectionNamey
```

Example: set d1 disable = hostb1,hostb2

3. Verify removal of host access with the following CLI command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 16.

Example Display 16

```
BuildngBTop> show units full  
-----  
LUN                               Uses                               Used by  
-----  
D1                                 DISK10000                          BUILDNGB\RCS1  
LUN ID:        6000-1FE1-0000-4250-0009-9411-5654-003E  
NOIDENTIFIER  
Switches:  
  RUN                               NOWRITE_PROTECT                       READ_CACHE  
  READAHEAD_CACHE                   WRITEBACK_CACHE  
  MAX_READ_CACHED_TRANSFER_SIZE = 32  
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32  
Access:  
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD,
```



```

State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = THIS_CONTROLLER
Size:      17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
D2          DISK20000          BUILDNGB\RCS2
LUN ID:      6000-1FE1-0000-4250-0009-9411-5654-003F
NOIDENTIFIER
Switches:
  RUN          NOWRITE_PROTECT          READ_CACHE
  READAHEAD_CACHE  WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = OTHER_CONTROLLER
Size:      17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )

```

- ④ 4. If your remote copy sets are set for asynchronous operation mode, switch to synchronous mode using the following CLI command:

```
SET RemoteCopySetName OPERATION_MODE = SYNCHRONOUS
```

```
Example: set rcs1 operation_mode = synchronous
```

Repeat this step for all remote copy sets.

- ④ 5. Continue Maintenance Failback at the initiator site with the Initiator Site Return Control Procedure, in the next section.

Initiator Site Return Control Procedure

This section describes how to return Data Replication Manager control to the initiator site.

- ▶ 1. Disconnect controller access with the following CLI commands:

```
SET THIS_CONTROLLER PORT_2_TOPOLOGY = OFFLINE
```

```
SET OTHER_CONTROLLER PORT_2_TOPOLOGY = OFFLINE
```

- ▶ 2. Verify that controller access was successfully disconnected by issuing the following CLI commands:

```
SHOW THIS_CONTROLLER
```

```
SHOW OTHER_CONTROLLER
```

You will see a display similar to that in Example Display 17.

Example Display 17

```
BuildngATop> show this_controller
Controller:
  HSG80 ZG84906303 Software V86-1P, Hardware E03
  NODE_ID          = 5000-1FE1-0000-01F0
  ALLOCATION_CLASS  = 0
  SCSI_VERSION     = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG84906237
  In dual-redundant configuration
  Device Port SCSI address 7
  Time: 10-MAY-2001 17:55:29
  Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-01F3
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address          = 220213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-01F4
  PORT_2_TOPOLOGY = OFFLINE (offline)
  REMOTE_COPY     = BUILDNGA
.
.
.
BuildngATop> show other_controller
Controller:
  HSG80 ZG84906237 Software V86-1P, Hardware E03
  NODE_ID          = 5000-1FE1-0000-01F0
  ALLOCATION_CLASS  = 0
  SCSI_VERSION     = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG84906303
  In dual-redundant configuration
  Device Port SCSI address 6
  Time: 10-MAY-2001 17:55:39
  Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-01F1
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address          = 250213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-01F2
  PORT_2_TOPOLOGY = OFFLINE (offline)
  REMOTE_COPY     = BUILDNGA
.
.
.
```

- ▶ 3. Fail back the initiator role to the initiator site with the following CLI command:

```
SITE_FAILOVER TargetRemoteCopyName\RemoteCopySetName
```

Example: `site_failover buildngB\rctl`

You will see a confirmation message, as shown in Example Display 18.

Example Display 18

```
%EVL--BuildngATop> --10-MAY-2001 17:57:17-- Instance Code: 0E010064
Template: 144.(90)
```

```

:
:
Instance Code: 0E010064

```

Repeat this step for each remote copy set.

- ▶ 4. Continue Maintenance Failback at the target site with the Target Site Restore Procedure.

Target Site Restore Procedure

- ⊙ 1. Turn off write history logging, if enabled, with the following CLI command:

```
SET AssociationSetName NOLOG_UNIT
```

```
Example: set as_d1 nolog_unit
```

Repeat this procedure for each association set.

- ⊙ 2. Delete the association set with the following CLI command:

```
DELETE AssociationSetName
```

```
Example: delete as_d1
```

Repeat this procedure for each association set.

- ⊙ 3. Delete all remote copy sets with following CLI command:

```
DELETE RemoteCopySetName
```

```
Example: delete rcs1
```

You will see a confirmation message, as shown in Example Display 19.

Example Display 19

```
BuildngBTop> delete rcs1
```

```
%EVL--BuildngBTop> --10-MAY-2001 18:01:12-- Instance Code: 0E020064
```

```
Template: 144.(90)
```

```
.
```

```
.
```

```
Remote Copy Set Name: "RCS1"
```

- ⊙ 4. Set the maximum cached transfer size to 128 with the following CLI command:

```
SET UnitName MAXIMUM_CACHED_TRANSFER_SIZE = 128
```

```
Example: set d1 maximum_cached_transfer_size = 128
```

Repeat this step for all initiator remote copy set units.

NOTE: This command sets both the read and write maximum cached transfer size.

- 5. Verify that maximum cached transfer size was set to 128 with the following CLI command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 20.

Example Display 20

```
BuildngBTop> show units full
-----
LUN                               Uses                               Used by
-----
D1                                  DISK10000
LUN ID:        6000-1FE1-0000-4250-0009-9411-5654-003E
NOIDENTIFIER
Switches:
  RUN          NOWRITE_PROTECT          READ_CACHE
  READAHEAD_CACHE  WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 128
  MAX_WRITE_CACHED_TRANSFER_SIZE = 128
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD
State:
  ONLINE to this controller
  PREFERRED_PATH = THIS_CONTROLLER
Size:        17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )

D2                                  DISK20000
LUN ID:        6000-1FE1-0000-4250-0009-9411-5654-003F
NOIDENTIFIER
Switches:
  RUN          NOWRITE_PROTECT          READ_CACHE
  READAHEAD_CACHE  WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 128
  MAX_WRITE_CACHED_TRANSFER_SIZE = 128
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD
State:
  ONLINE to the other controller
  PREFERRED_PATH = OTHER_CONTROLLER
Size:        17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
```

- 6. Continue Maintenance Failback at the initiator site with the Initiator Site Restoration of Target Connections Procedure.

Initiator Site Restoration of Target Connections Procedure

This section describes how to restore all target connections from the initiator site.

- 1. To restore the connections to the target site, enter the following CLI commands:

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

You will see a confirmation message, as shown in Example Display 21.

Example Display 21

```
%EVL--BuildngATop> --10-MAY-2001 18:05:11-- Instance Code: 0E120064
Template: 144.(90)
.
.
Instance Code: 0E120064
```

- ▶ 2. Enter the following commands to verify that the connections have been restored:

```
SHOW THIS_CONTROLLER
SHOW OTHER_CONTROLLER
```

You will see a display similar to that in Example Display 22.

Example Display 22

```
BuildngATop> show this_controller
Controller:
HSG80 ZG84906303 Software V86-1P, Hardware E03
NODE_ID = 5000-1FE1-0000-01F0
ALLOCATION_CLASS = 0
SCSI_VERSION = SCSI-3
Configured for MULTIBUS_FAILOVER with ZG84906237
In dual-redundant configuration
Device Port SCSI address 7
Time: 10-MAY-2001 18:05:38
Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
Reported PORT_ID = 5000-1FE1-0000-01F3
PORT_1_TOPOLOGY = FABRIC (fabric up)
Address = 220213
Host PORT_2:
Reported PORT_ID = 5000-1FE1-0000-01F4
PORT_2_TOPOLOGY = FABRIC (fabric up)
Address = 220413
REMOTE_COPY = BUILDNGA
.
.
BuildngATop> show other_controller
Controller:
HSG80 ZG84906237 Software V86-1P, Hardware E03
NODE_ID = 5000-1FE1-0000-01F0
ALLOCATION_CLASS = 0
SCSI_VERSION = SCSI-3
Configured for MULTIBUS_FAILOVER with ZG84906303
In dual-redundant configuration
Device Port SCSI address 6
Time: 10-MAY-2001 18:05:48
Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
Reported PORT_ID = 5000-1FE1-0000-01F1
PORT_1_TOPOLOGY = FABRIC (fabric up)
Address = 250213
```

```

Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-01F2
  PORT_2_TOPOLOGY = FABRIC (fabric up)
  Address          = 250413
  REMOTE_COPY     = BUILDNGA
.
.
.

```

- ▶ 3. Re-enable failsafe mode, if desired. To set failsafe mode, enter the following CLI command:

```
SET RemoteCopySetName ERROR_MODE = FAILSAFE
```

Example: `set rcs1 error_mode = failsafe`

Repeat this step for all applicable remote copy sets.

NOTE: Failsafe cannot be set if the remote copy set is in an association set that will be used for write history logging.

- ▶ 4. If you changed an asynchronous remote copy set to synchronous during failover, change it back to asynchronous mode with the following CLI command:

```
SET RemoteCopySetName OPERATION_MODE = ASYNCHRONOUS
```

Example: `set rcs1 operation_mode = asynchronous`

Repeat this step for all applicable remote copy sets.

- ▶ 5. Create association sets and then add the log unit, if desired. For information on how to create association sets, with or without write history logging, see Appendix C.

IMPORTANT: If you will be using scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention (remote copy sets, stripesets, mirrorsets, RAIDsets, association sets, and connections)—use underscores instead. Dashes are not allowed by the Perl scripting language.

Verify the log units with the following command:

```
SHOW ASSOCIATIONS FULL
```

You will see a display similar to that in Example Display 23.

Example Display 23

```

BuildngATop> show associations full
Name          Association          Uses          Used by
-----
AS_D1         association          RCS1
                                     RCS2

Switches:
NOFAIL_ALL
NOORDER_ALL

```

LOG_UNIT = D10 (No data logged)

- ▶ 6. Enable host access to all units used by remote copy sets at the initiator site, with the following CLI command:

```
SET UnitName ENABLE = InitiatorHostConnectionNamex,
InitiatorHostConnectionNamey
```

Example: set d1 enable = hosta1,hosta2

- ▶ 7. Verify that the initiator host can connect to the remote copy set units with this command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 24. In the Access field of the display, all remote copy set units will show that the initiator hosts are enabled.

Example Display 24

```
BuildngATop> show units full
-----
```

LUN	Uses	Used by
D1	DISK10000	BUILDNGA\RCS1
LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0134 NOIDENTIFIER Switches: RUN NOWRITE_PROTECT READ_CACHE READAHEAD_CACHE WRITEBACK_CACHE MAX_READ_CACHED_TRANSFER_SIZE = 32 MAX_WRITE_CACHED_TRANSFER_SIZE = 32 Access: BUILDNGBA, BUILDNGBB, BUILDNGBC, BUILDNGBD, HOSTA1, HOSTA2 State: ONLINE to the other controller PREFERRED_PATH = THIS_CONTROLLER Size: 17769177 blocks Geometry (C/H/S): (5258 / 20 / 169)		
D2	DISK20000	BUILDNGA\RCS2
LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0135 NOIDENTIFIER Switches: RUN NOWRITE_PROTECT READ_CACHE READAHEAD_CACHE WRITEBACK_CACHE MAX_READ_CACHED_TRANSFER_SIZE = 32 MAX_WRITE_CACHED_TRANSFER_SIZE = 32 Access: BUILDNGBA, BUILDNGBB, BUILDNGBC, BUILDNGBD HOST A1, HOSTA2 State: ONLINE to the other controller PREFERRED_PATH = OTHER_CONTROLLER Size: 17769177 blocks Geometry (C/H/S): (5258 / 20 / 169)		

- ▶ 8. Obtain your record of SHOW command output that details the original initiator configuration. Using the output as a reference, set the maximum cached transfer size to the original initiator value using the following CLI command:

```
SET UnitName MAXIMUM_CACHED_TRANSFER_SIZE = InitiatorValue
```

```
Example: set d1 maximum_cached_transfer_size = 32
```

Repeat this step for all remote copy set units.

NOTE: The default setting for maximum_cache_transfer_size is 32.

- ▶ 9. Allow hosts to recognize new units. Follow the steps listed below for each operating system in your heterogeneous configuration:

- a. **Compaq OpenVMS:** If the initiator site hosts are shut down, boot them now. Booting the hosts enables OpenVMS to recognize the drives.

If the initiator site hosts are not shut down, use the following command from a privileged account to enable OpenVMS to recognize the drives:

```
MCR SYSMAN IO AUTOCONFIGURE/LOG
```

- b. **Compaq Tru64 UNIX:** If the initiator site hosts are shut down, boot them now. Booting the hosts enables Tru64 UNIX to recognize the drives.

If the initiator site hosts are not shut down, use the following command to recognize the drives:

```
hwmgr - scan scsi
```

This might take a while for large configurations. If this is the case, scan only those SCSI buses that have new units added. Scan only one bus at a time. Use the following command:

```
hwmgr -scan scsi -bus x
```

where x is the SCSI bus number.

- c. **HP-UX:** If the initiator site hosts are shut down, boot them now. Booting the hosts enables HP-UX to recognize the drives.

If the initiator site hosts are not shut down, use the following commands to recognize the drives and mount the file systems:

```
ioscan -fnCdisk
```

```
mount -a
```

- d. **IBM AIX:** If the initiator site hosts are shut down, boot them now. Booting the hosts enables IBM AIX to recognize the drives.

If the initiator site hosts are not shut down, use the following commands to recognize the drives and mount the file systems:

```
cfgmgr -v  
mount all
```

- e. **Microsoft Windows NT-X86:** Reboot the hosts at the initiator site and log in using an account that has administrative privileges. You should be able to see all of the units by choosing **My Computer**.

- f. **Microsoft Windows 2000:**

- 1) If you *have not* changed the UNIT_OFFSET of any host connections since the hosts have been booted, you do not need to reboot the initiator site hosts.

- a) On each host, log in using an account that has administrative privileges.

- b) Open **Computer Management** and click **Disk Management**.

- c) After **Disk Management** has initialized, go to the **Action** menu and click **Rescan Disks**. All of the failed over units should appear in the right-hand pane. If Secure Path is not installed correctly, you will see each unit twice.

- 2) If you *have* changed the UNIT_OFFSET of any host connections, you must reboot that host. After the server has rebooted, log in using an account that has administrative privileges. You will see all of the units in **Computer Management > Disk Management**. If Secure Path is not installed correctly, you will see each drive twice.

- g. **Novell NetWare:** If the initiator site hosts are shut down, boot them now. Booting the hosts allows Novell NetWare to recognize the drives.

If the initiator site hosts are already up and running, or if they do not recognize the drives, issue the following command from the console before mounting the volumes:

```
SCAN FOR NEW DEVICES
```

Alternatively, you can use the `nwCONFIG` utility to issue this same command.

- h. **SUN Solaris:** Reboot the hosts using the command `reboot -- -r` at the initiator site and log in using an account that has administrative privileges. You should be able to see all of the units by using the `format` command.

If Secure Path was not configured for these units, you will not see the drives. You will need to edit the WWLIDs in the file `/kernel/drv/ldLite.conf`. To find the new WWLIDs of the units, use the `SHOW Unitname` command on the controller. You may also need to adjust the files `/kernel/drv/mda.conf` and `/kernel/drv/sd.conf` to accommodate the extras LUNs. When you have edited `ldLite.conf`, `mda.conf`, and `sd.conf`, reboot the host using the `reboot -- -r` command. You should now be able to see the drives using the `format` command. Refer to the *Compaq SANworks Secure Path for Sun Solaris Installation and Reference Guide* for additional assistance.

This completes the Extended Planned Site Failover with Full Failback.

Resumption of Replication After Extended Planned Loss of Target Procedure (Failsafe Mode)

Use this procedure when the error mode of the remote copy sets is set for failsafe and the target site will be shut down for an extended length of time. Setting the remote copy set's error mode to normal allows host I/O to continue while the target site is offline. Because there is no log unit configured, a full copy will be performed once the target site is back online.

Every command in this procedure should be performed only for those remote copy sets in your configuration with error mode set to failsafe.

This chapter contains these procedures for resuming replication due to an extended loss of the target:

- “Prepare Remote Copy Sets” on page 8–2
- “Target Site Availability” on page 8–4
- “Resume Remote Copy Set Operation” on page 8–4

NOTE: In this chapter, *initiator* site procedure steps are identified by an arrow symbol ► in the margin. *Target* site procedure steps are identified by a target symbol Ⓣ in the margin.

NOTE: Some example displays illustrate confirmation messages with the event log symbol (%EVL) and an instance code. Compare the instance code in the example with the instance code you receive. If the numbers are the same, you have performed the previous command correctly and have achieved the desired results. Note that you will be able to see these screens only if you are working from the controller to which the LUNs are online. Refer to the Troubleshooting chapter for more information on instance codes and their meanings.

Example displays may also contain bold text to identify information that is the most pertinent in the example. In many cases, items shown in bold text will help you verify the results of a previous command.

Prepare Remote Copy Sets

- ▶ 1. Use the following CLI command to verify that the error mode of the remote copy sets is set to failsafe:

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to that in Example Display 1.

Example Display 1

```
BuildngATop> show remote_copy_sets full
Name                               Uses                               Used by
-----
RCS1      remote copy                       D1                               AS_D1
Reported LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003E
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE = FAILSAFE
  FAILOVER_MODE = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGA\D1) state:
  ONLINE to this controller
  Not reserved
Target state:
  BUILDNGB\D1      is NORMAL
```

- ▶ 2. Set the error mode of the remote copy sets to normal with the following CLI command:

```
SET RemoteCopySetName ERROR_MODE = NORMAL
```

Example: `set rcs1 error_mode = normal`

Repeat this step for all applicable remote copy sets.

- ▶ 3. Use the following CLI command to verify that the error mode of the remote copy sets is normal:

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to that in Example Display 2.

Example Display 2

```
BuildngATop> show remote_copy_sets full
Name                               Uses                               Used by
-----
RCS1      remote copy                    D1                               AS_D1
Reported LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003E
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE = NORMAL
  FAILOVER_MODE = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGA\D1) state:
  ONLINE to this controller
  Not reserved
Target state:
  BUILDNGB\D1      is NORMAL
```

- ▶ 4. Remove the targets with the following CLI command:

```
SET RemoteCopySetName REMOVE = TargetRemoteCopyName\UnitName
```

Example: set rcs1 remove = buildngB\d1

You will see a confirmation message, as shown in Example Display 3.

Example Display 3

```
BuildngATop> set rcs1 remove = buildngB\d1

%EVL--BuildngATop> --10-MAY-2001 16:49:55-- Instance Code: 0E078A01
Template: 144.(90)
.
.
.
Instance Code: 0E078A01
```

Repeat this step for all applicable remote copy sets.

- ▶ 5. Verify that you have removed the targets by entering the following CLI command:

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to that in Example Display 4.

Example Display 4

```
BuildngATop> show remote_copy_sets full
Name                               Uses                               Used by
-----
RCS1      remote copy                       D1
Reported LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0134
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGA\D1) state:
  ONLINE to the other controller
No targets
```

Target Site Availability

- ⦿ The target site is now available for desired actions.
- ⦿ When the target site is operational and back on line, continue resumption of operations with the Resume Remote Copy Set Operation procedure. If the target site must be powered off, follow the procedure in Appendix B.

Resume Remote Copy Set Operation

- ▶ 1. If you are connected to the initiator site controllers when the target site comes online, you will see the following confirmation messages, as shown in Example Display 5.

Example Display 5

```
BuildngATop>
%EVL--BuildngATop> --07-JUN-2001 14:16:15-- Instance Code: 07050064
Template: 5.(05)
Power On Time: 2. Years, 73. Days, 6. Hours, 50. Minutes, 57. Seconds
Event reported by Peer to Peer Remote Copy target controller
Controller Model: HSG80
Serial Number: ZG94115654 Hardware Version: E10(28)
Software Version: V86-1P
Instance Code: 07050064
Last Failure Code: 08090010 (No Last Failure Parameters)

%EVL--BuildngATop> --07-JUN-2001 14:16:15-- Instance Code: 43010064
Template: 4.(04)
Power On Time: 2. Years, 73. Days, 6. Hours, 50. Minutes, 57. Seconds
Event reported by Peer to Peer Remote Copy target controller
Controller Model: HSG80
Serial Number: ZG94115654 Hardware Version: E10(28)
Software Version: V86-1P
```

```
Other Controller Serial Number: ZG94319198
Failed Controller Target Number: 0.(00)
LUNs Taken By This Controller:
00000003
00000000
00000000
00000000
00000000
00000000
00000000
00000000
00000000
Instance Code: 43010064
```

- ▶ 2. Add back the target to the initiator unit's remote copy sets with the following CLI command:

```
SET RemoteCopySetName ADD = TargetRemoteCopyName\UnitName
```

Example: set rcs1 add = buildingB\d1

You will see a confirmation message, as shown in Example Display 6.

Example Display 6

```
BuildngATop> set rcs1 add=buildngB\d1
%EVL--BuildngATop> --10-MAY-2001 17:37:27-- Instance Code: 0E050064
Template: 144.(90)
.
.
Instance Code: 0E050064
```

Repeat this step for all applicable remote copy sets.

NOTE: This command will cause the remote copy sets to begin normalization.

- ▶ 3. Enter the following command to see the percentage of normalization completion for all remote copy sets.

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to that in Example Display 7.

Example Display 7

```
BuildngATop> show remote_copy_sets full
Name                               Uses                               Used by
-----
RCS1      remote copy                    D1                               AS_D1
Reported LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0134
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGA\D1) state:
  ONLINE to the other controller
Target state:
BUILDNGB\D1      is COPYING          94% complete
```

```
BuildngATop> show remote_copy_sets full
Name                               Uses                               Used by
-----
RCS1      remote copy                    D1                               AS_D1
Reported LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0134
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGA\D1) state:
  ONLINE to the other controller
Target state:
BUILDNGB\D1      is NORMAL
```

When the units are all normalized, the Target field of the display will show NORMAL, as shown in the lower half of the example display.

IMPORTANT: Wait for normalization on all remote copy sets to complete before you proceed.

- ▶ 4. Set the error mode of the remote copy sets to failsafe with the following CLI command:

```
SET RemoteCopySetName ERROR_MODE = FAILSAFE
```

Example: `set rcs1 error_mode = failsafe`

Repeat this step for all applicable remote copy sets.

- ▶ 5. Use the following CLI command to verify that the error modes of the remote copy sets are set to failsafe:

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to that in Example Display 8.

Example Display 8

```
BuildngATop> show remote_copy_sets full
Name                               Uses                               Used by
-----
RCS1      remote copy                    D1                               AS_D1
Reported LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003E
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE = FAILSAFE
  FAILOVER_MODE = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGA\D1) state:
  ONLINE to this controller
  Not reserved
Target state:
  BUILDNGB\D1      is NORMAL
```

This completes the procedure for resuming of operations after an extended planned loss of the target.

Unplanned Site Failover with Failback to New Hardware Procedure

In this scenario a disaster of some type of disaster (lightening, flood, fire, or the like) has damaged the initiator site. You will perform an unplanned site failover to the target site. When the damaged components at the initiator site (hosts, controllers, switches, for example) have been repaired, and the site is operational and back online, you will perform a failback to the new hardware.

This chapter contains these procedures to ensure that an unplanned failover and subsequent failback function properly:

- “Unplanned Failover” on page 9–2
- “New Hardware Failback” on page 9–13

NOTE: In this chapter, *initiator* site procedure steps are identified by an arrow symbol ► in the margin. *Target* site procedure steps are identified by a target symbol ☉ in the margin.

NOTE: Some example displays illustrate confirmation messages with the event log symbol (%EVL) and an instance code. Compare the instance code in the example with the instance code you receive. If the numbers are the same, you have performed the previous command correctly and have achieved the desired results. Note that you will be able to see these screens only if you are working from the controller to which the LUNs are online. Refer to the Troubleshooting chapter for more information on instance codes and their meanings.

Example displays may also contain bold text to identify information that is the most pertinent in the example. In many cases, items shown in bold text will help you verify the results of a previous command.

Unplanned Failover

Use the Unplanned Failover in this section in conjunction with the New Hardware Failback procedures whenever a situation occurs at the initiator site to bring it down (unable to perform its functions as an initiator).

Target Site Failover Procedure

IMPORTANT: Since the initiator may be running (and perhaps write history logging), you must ensure that:

- The intersite connections are severed.
- You do not restore the connection until directed to do so in the proper failback procedure.

1. Verify that the intersite connections are severed with the following CLI command:

```
SHOW THIS_CONTROLLER
SHOW OTHER_CONTROLLER
```

You will see a display similar to that in Example Display 1.

Example Display 1

```
BuildngBTop> show this_controller
Controller:
  HSG80 ZG94115654 Software V86-1P, Hardware E10
  NODE_ID           = 5000-1FE1-0000-4250
  ALLOCATION_CLASS   = 0
  SCSI_VERSION      = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG94319198
  In dual-redundant configuration
  Device Port SCSI address 7
  Time: 10-MAY-2001 16:41:11
  Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-4253
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address          = 260213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-4254
  PORT_2_TOPOLOGY = FABRIC (connection down)
  Address          = 260413
  REMOTE_COPY     = BUILDNGB
.
.
.
BuildngBTop> show other_controller
Controller:
  HSG80 ZG94319198 Software V86-1P, Hardware E10
  NODE_ID           = 5000-1FE1-0000-4250
  ALLOCATION_CLASS   = 0
  SCSI_VERSION      = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG94115654
  In dual-redundant configuration
  Device Port SCSI address 6
  Time: 10-MAY-2001 16:43:12
```

```

Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-4251
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address          = 200213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-4252
  PORT_2_TOPOLOGY = FABRIC (connection down)
  REMOTE_COPY     = BUILDNGB
.
.
.

```

2. Ensure that the connection between sites is not restored by entering the following CLI commands:

```

SET THIS_CONTROLLER PORT_2_TOPOLOGY = OFFLINE
SET OTHER_CONTROLLER PORT_2_TOPOLOGY = OFFLINE

```

3. Verify the lack of connection with the following CLI commands:

```

SHOW THIS_CONTROLLER
SHOW OTHER_CONTROLLER

```

You will see a display similar to that in Example Display 2.

Example Display 2

```

BuildngBTop> show this_controller
Controller:
  HSG80 ZG94115654 Software V86-1P, Hardware E10
  NODE_ID          = 5000-1FE1-0000-4250
  ALLOCATION_CLASS  = 0
  SCSI_VERSION     = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG94319198
  In dual-redundant configuration
  Device Port SCSI address 7
  Time: 10-MAY-2001 16:42:49
  Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-4253
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address          = 260213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-4254
  PORT_2_TOPOLOGY = OFFLINE (offline)
  REMOTE_COPY     = BUILDNGB
.
.
.
BuildngBTop> show other_controller
Controller:
  HSG80 ZG94319198 Software V86-1P, Hardware E10
  NODE_ID          = 5000-1FE1-0000-4250
  ALLOCATION_CLASS  = 0
  SCSI_VERSION     = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG94115654

```

```

        In dual-redundant configuration
        Device Port SCSI address 6
        Time: 10-MAY-2001 16:43:12
        Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
    Reported PORT_ID = 5000-1FE1-0000-4251
    PORT_1_TOPOLOGY = FABRIC (fabric up)
    Address          = 200213
Host PORT_2:
    Reported PORT_ID = 5000-1FE1-0000-4252
    PORT_2_TOPOLOGY = OFFLINE (offline)
    REMOTE_COPY = BUILDNGB
.
.
.

```

- ④ 4. At the target site, the remote copy set units must be preferred to one controller or the other.
 - a. Use the following CLI command to check for the preferred path:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 3.

Example Display 3

```

BuildngBTop> show units full
-----
LUN                               Uses                               Used by
-----
D1                                  DISK10000                          BUILDNGA\RCS1
LUN ID:        6000-1FE1-0000-4250-0009-9411-5654-003E
NOIDENTIFIER
Switches:
  RUN          NOWRITE_PROTECT      READ_CACHE
  READAHEAD_CACHE  WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 128
  MAX_WRITE_CACHED_TRANSFER_SIZE = 128
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD
State:
  ONLINE to the other controller
  PREFERRED_PATH = THIS_CONTROLLER
  Target NORMAL
Size:          17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
D2                                  DISK20000                          BUILDNGA\RCS2
LUN ID:        6000-1FE1-0000-4250-0009-9411-5654-003F
NOIDENTIFIER
Switches:
  RUN          NOWRITE_PROTECT      READ_CACHE
  READAHEAD_CACHE  WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD
State:
  ONLINE to this controller
  Not reserved

```

```

PREFERRED_PATH = OTHER_CONTROLLER
Target NORMAL
Size: 17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
    
```

- b. If the remote copy set units are not currently preferred, use the following CLI command:

```
SET UnitName PREFERRED_PATH = THIS_CONTROLLER
```

```
Example: set d1 preferred_path = this_controller
```

or

```
SET UnitName PREFERRED_PATH = OTHER_CONTROLLER
```

```
Example: set d2 preferred_path = other_controller
```

Repeat this step for each remote copy set unit that needs to be preferred.

5. Use the following CLI command to failover each remote copy set (maximum of 12 per subsystem):

```
SITE_FAILOVER InitiatorRemoteCopyName\RemoteCopySetName
```

```
Example: site_failover buildngA\rsc1
```

You will see a confirmation message, as shown in Example Display 4.

Example Display 4

```
BuildngBTop> site_failover buildngA\rsc1
```

```
%EVL--BuildngBTop> --10-MAY-2001 16:48:08-- Instance Code: 0E010064
```

```
Template: 144.(90)
```

```
.
.
.
```

```
Instance Code: 0E010064
```

Repeat this step for all remote copy sets.

6. Remove the targets with the following CLI command:

```
SET RemoteCopySetName REMOVE = InitiatorRemoteCopyName\UnitNumber
```

```
Example: set rsc1 remove = buildngA\d1
```

You will see a confirmation message, as shown in Example Display 5.

Example Display 5

```
BuildngBTop> set rcs1 remove=buildngA\d1

%EVL--BuildngBTop> --10-MAY-2001 16:49:55-- Instance Code: 0E078A01
Template: 144.(90)
.
.
.
Instance Code: 0E078A01
```

Repeat this step for all remote copy sets.

7. Verify the removal of the targets with the following CLI command:

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to that in Example Display 6.

Example Display 6

```
BuildngBTop> show remote_copy_sets full
Name                                     Uses                                Used by
-----
RCS1      remote copy                            D1
Reported LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0134
Switches:
OPERATION_MODE = SYNCHRONOUS
ERROR_MODE     = NORMAL
FAILOVER_MODE  = MANUAL
OUTSTANDING_IOS = 20
Initiator (BUILDNGB\D1) state:
ONLINE to the other controller
Not reserved
No targets
```

8. Obtain your record of `SHOW` command output that details the original initiator configuration. Using the output as a reference, create association sets to duplicate those that were on the initiator. For information on how to create association sets, see Appendix C.

IMPORTANT: If you will be using scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention (remote copy sets, stripesets, mirrorsets, RAIDsets, association sets, and connections)—use underscores instead. Dashes are not allowed by the Perl scripting language.

Repeat this step for each applicable association set. You can set up write history logging after targets are added back to the configuration later in this chapter.

- 9. Enable host access to all remote copy set units at the target site with the following CLI command:

```
SET UnitName ENABLE = TargetHostConnectionNamex,  
TargetHostConnectionNamey
```

Example: set d1 enable = hostb1,hostb2

You will see a display similar to that in Example Display 7.

Example Display 7

```
BuildngBTop> set d1 enable=hostb1,hostb2  
Warning 1000: Other host(s) in addition to the one(s) specified can still  
access this unit. If you wish to enable ONLY the host(s)  
specified, disable all access paths (DISABLE_ACCESS=ALL), then  
again enable the ones specified
```

Repeat this step for each remote copy set unit.

- 10. If you do not recall a target host connection name, use the following command:

```
SHOW CONNECTIONS
```

You will see a display similar to that in Example Display 8.

Example Display 8

```
BuildngBTop> show connections
```

Connection Name	Operating system	Controller	Port	Address	Status	Unit Offset
BUILDNGAA	PPRC_TARGET HOST_ID=5000-1FE1-0000-01F0	THIS	2		offline	0
BUILDNGAB	PPRC_TARGET HOST_ID=5000-1FE1-0000-01F0	OTHER	2		offline	0
BUILDNGAC	PPRC_INITIATOR HOST_ID=5000-1FE1-0000-01F0	THIS	2	220413	offline	0
BUILDNGAD	PPRC_INITIATOR HOST_ID=5000-1FE1-0000-01F0	OTHER	2	250413	offline	0
HOSTA1	WINNT HOST_ID=1000-0000-C920-A7B9	THIS	1	260013	OL this	0
HOSTA2	WINNT HOST_ID=1000-0000-C921-3F4E	OTHER	1	200013	OL other	0
HOSTB1	WINNT HOST_ID=1000-0000-C921-3E98	THIS	1	220013	OL this	0
HOSTB2	WINNT HOST_ID=1000-0000-C921-3EFC	OTHER	1	250013	OL other	0

- ① 11. Verify the target site hosts access with the following CLI command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 9.

Example Display 9

```
BuildngBTop> show units full
-----
LUN                               Uses                               Used by
-----
D1                                  DISK10000                          BUILDNGB\RCS1
  LUN ID:      6000-1FE1-0000-4250-0009-9411-5654-003E
  NOIDENTIFIER
  Switches:
    RUN                NOWRITE_PROTECT          READ_CACHE
    READAHEAD_CACHE    WRITEBACK_CACHE
    MAX_READ_CACHED_TRANSFER_SIZE = 32
    MAX_WRITE_CACHED_TRANSFER_SIZE = 32
  Access:
    BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD,  HOSTB1,  HOSTB2
  State:
    ONLINE to this controller
    Not reserved
    PREFERRED_PATH = THIS_CONTROLLER
  Size:          17769177 blocks
  Geometry (C/H/S): ( 5258 / 20 / 169 )

D2                                  DISK20000                          BUILDNGB\RCS2
  LUN ID:      6000-1FE1-0000-4250-0009-9411-5654-003F
  NOIDENTIFIER
  Switches:
    RUN                NOWRITE_PROTECT          READ_CACHE
    READAHEAD_CACHE    WRITEBACK_CACHE
    MAX_READ_CACHED_TRANSFER_SIZE = 32
    MAX_WRITE_CACHED_TRANSFER_SIZE = 32
  Access:
    BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD,  HOSTB1,  HOSTB2
  State:
    ONLINE to this controller
    Not reserved
    PREFERRED_PATH = OTHER_CONTROLLER
  Size:          17769177 blocks
  Geometry (C/H/S): ( 5258 / 20 / 169 )
```

In the Access field of the display, all units that are used by remote copy sets will show that both the target host and the initiator controller connections are enabled.

- ① 12. If you wish, you can enhance host I/O performance by resetting the maximum cached transfer size to the original value used on the initiator. Obtain your record of SHOW command output that details the original initiator configuration. Using the output as a reference, set the maximum cached transfer size to the original initiator value using the following CLI command:

```
SET UnitName MAXIMUM_CACHED_TRANSFER_SIZE = InitiatorValue
```

```
Example: set d1 maximum_cached_transfer_size = 32
```

Repeat this step for all remote copy set units.

- ① 13. Verify that you have set the maximum cached transfer size to 32 with the following CLI command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 10.

Example Display 10

```
BuildngBTop> show units full
-----
LUN                               Uses                               Used by
-----
D1                                DISK10000                          BUILDNGB\RCS1
LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003E
NOIDENTIFIER
Switches:
  RUN                               NOWRITE_PROTECT                     READ_CACHE
  READAHEAD_CACHE                   WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD,  HOSTB1,  HOSTB2
State:
  ONLINE to the other controller
  PREFERRED_PATH = THIS_CONTROLLER
Size: 17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )

D2                                DISK20000                          BUILDNGA\RCS2
LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003F
NOIDENTIFIER
Switches:
  RUN                               NOWRITE_PROTECT                     READ_CACHE
  READAHEAD_CACHE                   WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = OTHER_CONTROLLER
  Target NORMAL
Size: 17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
```

NOTE: The default value for maximum cached transfer size is 32.

- ① 14. If, while performing failover, you decided to create a new unit protected by a new remote copy set, use the following CLI command:

```
ADD REMOTE_COPY_SETS RemoteCopySetName UnitName
```

Example: add remote_copy_sets rcs3 d3

The target will be added at failback.

IMPORTANT: If you will be using scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention (remote copy sets, stripesets, mirrorsets, RAIDsets, association sets, and connections)—use underscores instead. Dashes are not allowed by the Perl scripting language.

- ① 15. Allow hosts to recognize new units. Follow the steps listed below for each operating system in your heterogeneous configuration:

- a. **Compaq OpenVMS:** If the target site hosts are shut down, boot them now. Booting the hosts enables OpenVMS to recognize the drives.

If the target site hosts are not shut down, use the following command from a privileged account to enable OpenVMS to recognize the drives:

```
MCR SYSMAN IO AUTOCONFIGURE/LOG
```

- b. **Compaq Tru64 UNIX:** If the target site hosts are shut down, boot them now. Booting the hosts enables Tru64 UNIX to recognize the drives.

If the target site hosts are not shut down, use the following command to recognize the drives:

```
hwmgr - scan scsi
```

This might take a while for large configurations. If this is the case, scan only those SCSI buses that have new units added. Scan only one bus at a time. Use the following command:

```
hwmgr -scan scsi -bus x
```

where x is the SCSI bus number.

- c. **HP-UX:**

- 1) If the target site hosts are shut down, boot them now. Booting the hosts enables HP-UX to recognize the drives.

If the target site hosts are not shut down, use the following command to enable HP-UX to recognize the drives and verify that they are present. This command will display only the previously configured failed-over LUNs:

```
ioscan -fnCdisk
```

- 2) Continue with the following commands to access file systems on new failed-over LUNs. If you have no new failed-over LUNs, skip these substeps and go directly to the next step to mount the LUNs:

a. `/opt/CPQswsp/spmgr display -u`

b. `/opt/CPQswsp/spmgr add WWN`

Repeat this command for each un-attached WWN that was displayed.

c. `ioscan -fnCdisk`

If the device special files were not displayed, run `insf -e`, then run `ioscan -fnCdisk` again.

d. `vgimport VolumeGroupName DeviceSpecialFile`

Repeat this command for each new failed-over LUN.

3) Use the following command to mount the LUNs:

```
mount -a
```

NOTE: *VolumeGroupName* is the name of the volume group you originally created at the initiator site. The *DeviceSpecialFiles* are from the `ioscan` in the form of `/dev/dsk/c_t_d_`.

For consistency, configure the same *DeviceSpecialFiles* with the same volume groups, logical volumes, and file systems for the failed-over LUNs at the target site with the same LUNs at the initiator site.

d. **IBM AIX:** If the target site hosts are shut down, boot them now. Booting the hosts enables IBM AIX to recognize the drives.

If the target site hosts are not shut down, use the following commands to enable AIX to recognize the drives and verify that they are present:

```
cfgmgr -v
```

```
lsdev -Cc disk
```

Use the following commands to access file systems on the failed-over LUNs:

```
importvg -y volumegroupname hdiskx
```

```
mount all
```

NOTE: *volumegroupname* is the name of the volume group you originally created at the initiator site, and *x* is the number of the `hdisk` assigned to the failed-over LUN. If the `-y volumegroupname` parameter is omitted, AIX will create a default volume group name for you, for example, `vg00`.

e. **Microsoft Windows NT-X86:** Reboot the hosts at the target site and log in using an account that has administrative privileges. You should be able to see all of the units by choosing **My Computer**.

f. **Microsoft Windows 2000:**

1) If you *have not* changed the `UNIT_OFFSET` of any host connections since the hosts have been booted, you do not need to reboot the initiator site hosts.

a) On each host, log in using an account that has administrative privileges.

- b) Open **Computer Management** and click **Disk Management**.
 - c) After **Disk Management** has initialized, go to the **Action** menu and click **Rescan Disks**. All of the failed over units should appear in the right-hand pane. If Secure Path is not installed correctly, you will see each unit twice.
- 2) If you *have* changed the UNIT_OFFSET of any host connections, you must reboot that host. After the server has rebooted, log in using an account that has administrative privileges. You will see all of the units in **Computer Management > Disk Management**. If Secure Path is not installed correctly, you will see each drive twice.
- g. **Novell NetWare:** If the target site hosts are shut down, boot them now. If you are using traditional NetWare volumes, booting the hosts allows Novell NetWare to recognize the drives and automatically mount the volumes. If you are using NSS logical volumes, booting the hosts will recognize the NSS pools and activate them. However, you must manually mount each individual NSS volume by typing `MOUNT VolumeName` at the NetWare console.

If the target site hosts are already up and running, or if they do not recognize the drives, issue the following command from the console before mounting the volumes:

```
SCAN FOR NEW DEVICES
```

Alternatively, you can use the `NWCONFIG` utility to issue this same command.

Next, mount the volumes with these commands:

```
MOUNT ALL (for traditional NetWare volumes)
```

```
MOUNT VolumeName (for NSS logical volumes).
```

- h. **SUN Solaris:** Reboot the hosts using the command `reboot -- -r` at the target site and log in using an account that has administrative privileges. You should be able to see all of the units by using the `format` command.

If Secure Path was not configured for these units, you will not see the drives. You will need to edit the WWLIDs in the file `/kernel/drv/ldLite.conf`. To find the new WWLIDs of the units, use the `SHOW Unitname` command on the controller. You may also need to adjust the files `/kernel/drv/mda.conf` and `/kernel/drv/sd.conf` to accommodate the extras LUNs. When you have edited `ldLite.conf`, `mda.conf`, and `sd.conf`, reboot the host using the `reboot -- -r` command. You should now be able to see the drives using the `format` command. Refer to the *Compaq SANworks Secure Path for Sun Solaris Installation and Reference Guide* for additional assistance.

This completes the Unplanned Failover. When the initiator systems have been replaced, or the problems that disabled the initiator site have been remedied, continue with New Hardware Failback in the next section.

New Hardware Failback

Use New Hardware Failback when *any storage hardware at the initiator site has been replaced, and the new hardware is not configured.*

The New Hardware Failback consists of the following procedures:

- Initiator Site Preparation Procedure
- Target Site Preparation Procedure
- Initiator Site Connections Procedure
- Target Site Copy Data Procedure
- Initiator Site Return Control Procedure
- Target Site Restore Procedure
- Initiator Site Restoration of Target Connections Procedure

Initiator Site Preparation Procedure

- ▶ 1. Follow the steps listed below for each operating system in your heterogeneous configuration:
 - a. **Compaq OpenVMS:** If the operating system is up and running, and is being used exclusively for DRM operations, shut down the operating system and power off the hosts. If the operating system is being used for other applications, remove all I/O to the remote copy set LUNs that will be failed over, then dismount the volumes associated with these LUNs.
 - b. **Compaq Tru64 UNIX:** If the operating system is up and running and is being used exclusively for DRM operations, shut down the operating system and power off the hosts. If the operating system is being used for other applications, remove all I/O and unmount all file system LUNs that have remote copy sets that will be failed over.
 - c. **HP-UX:** If the operating system is up and running, remove all I/O to the remote copy set LUNs that will be failed over, then unmount the file systems associated with these LUNs.

- d. **IBM AIX:** If the operating system is up and running, remove all I/O to the remote copy set LUNs that will be failed over, then unmount the file systems associated with these LUNs.
- e. **Microsoft Windows NT-X86:** If the operating system is up and running, shut it down and power off the hosts.
- f. **Microsoft Windows 2000:** If the operating system is up and running, shut it down and power off the hosts.
- g. **Novell NetWare:** If the operating system is up and running, remove all I/O to the remote copy set LUNs that will be failed over, then dismount the volumes associated with these LUNs.

If you are using NetWare Cluster Services (NWCS), you must enter the `cluster down` command. You must also enter the `uldncs` (unload NetWare Cluster Services) command for all cluster nodes.



CAUTION: Failure to enter these two commands will cause all cluster nodes toabend.

- h. **SUN Solaris:** If the operating system is up and running and is being used exclusively for DRM operations, shut down the operating system and power off the hosts. If the operating system is being used for other applications, remove all I/O and unmount all volumes that have remote copy sets that will be failed over.
- ▶ 2. Obtain your record of `SHOW` command output that details the original initiator configuration. Using the output as a reference, manually reconfigure the controllers, but do not re-create the original remote copy sets.

NOTE: Steps step c, step f, and step g will cause the controller pair to restart.

- a. Set node ID and checksum for **THIS** controller. This information can be found on the original initiator controller rack. See the *SANworks Data Replication Manager by Compaq HSG80 ACS Version 8.6-4P Configuration User Guide* for information on the node ID and checksum.
The node ID for the **OTHER** controller will be set automatically by the command in step step c.

- b. **Compaq OpenVMS only:** Set the device ID to its previous value with the following command:

```
SET THIS IDENTIFIER = Value
```

Example: set this identifier = 98

Verify the identifier setting with the following command:

```
SHOW THIS_CONTROLLER
```

You will see a display similar to that in Example Display 11.

Example Display 11

```
HSG> show this_controller
Controller:
  HSG80 ZG84906303 Software V86-1P, Hardware E03
  NODE_ID           = 5000-1FE1-0000-01F0
  ALLOCATION_CLASS   = 0
  SCSI_VERSION      = SCSI-2
  Not configured for dual-redundancy
  Device Port SCSI address 7
  Time: 11-MAY-2001 11:41:36
  Command Console LUN is lun 0 (IDENTIFIER = 98)
.
.
.
```

- c. Configure the controllers for multiple bus failover mode by issuing the following CLI command:

```
SET MULTIBUS_FAILOVER COPY = THIS_CONTROLLER
```

This command will automatically restart the OTHER controller.

- d. (Optional) Set the controller to the preferred SCSI mode with the following CLI command:

```
SET THIS_CONTROLLER SCSI_VERSION = SCSI-x
```

where $x = 2$ or 3 .

SCSI-2 is the default setting.

NOTE: Do not restart the controller.

- e. Designate a controller prompt with the following CLI commands:

```
SET THIS_CONTROLLER PROMPT= "InitiatorControllerNameTop> "
```

Example: set this_controller prompt = "buildngA Top> "

```
SET OTHER_CONTROLLER PROMPT="InitiatorControllerNameBottom> "
```

Example: set other_controller prompt = "buildngA Bottom> "

- f. Set mirrored cache using the following CLI command:

```
SET THIS_CONTROLLER MIRRORED_CACHE
```

NOTE: This CLI command may fail because internal cache diagnostics are running. These diagnostics can take up to 5 minutes to complete, so you may need to retry this command.

- g. Enter the following command:

```
SET THIS_CONTROLLER REMOTE_COPY = InitiatorRemoteCopyName
```

Example: `set this_controller remote_copy = buildngA`

NOTE: The *InitiatorRemoteCopyName* must be the same as on the original controller hardware configuration

IMPORTANT: If you will be using scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention (remote copy sets, stripesets, mirrorsets, RAIDsets, association sets, and connections)—use underscores instead. Dashes are not allowed by the Perl scripting language.



- h. Run the Configuration utility to assign a disk name to physical disks with the following CLI command:

```
RUN CONFIG
```

You will see a display similar to that in Example Display 12.

Example Display 12

```
BuildngATop> run config
```

```
Config Local Program Invoked
```

```
Config is building its tables and determining what devices exist  
on the subsystem. Please be patient.
```

```
add disk DISK10000 1 0 0  
add disk DISK10100 1 1 0  
add disk DISK10200 1 2 0  
add disk DISK10300 1 3 0  
add disk DISK20000 2 0 0  
add disk DISK20100 2 1 0  
add disk DISK20200 2 2 0  
add disk DISK20300 2 3 0  
add disk DISK30000 3 0 0  
add disk DISK30100 3 1 0  
add disk DISK30200 3 2 0  
add disk DISK30300 3 3 0  
add disk DISK40000 4 0 0  
add disk DISK40300 4 3 0  
add disk DISK50000 5 0 0  
add disk DISK50300 5 3 0  
add disk DISK60000 6 0 0  
add disk DISK60300 6 3 0
```

```
Config - Normal Termination
```

- i. Using the configuration data from the target, create and initialize all storagesets and units. This includes all that had existed at the initiator site as well as those that were created at the target site since failover. The units that will be part of remote copy sets must be identical to the corresponding units at the target site. Wait to create any units that will be used for log disks until later in the chapter. See the *Compaq SANworks HSG80 ACS Version 8.6-4P Configuration Guide* for information on creating storagesets and units.

IMPORTANT: If you will be using scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention (remote copy sets, stripesets, mirrorsets, RAIDsets, association sets, and connections)—use underscores instead. Dashes are not allowed by the Perl scripting language.

- j. Verify the creation of the storagesets and units with the following CLI command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 13.

Example Display 13

```
BuildngATop> show units full
LUN                               Uses                               Used by
-----
d1                                  DISK10000
LUN ID:        6000-1FE1-0000-01F0-0009-8490-6303-0134
NOIDENTIFIER
Switches:
  RUN                NOWRITE_PROTECT                READ_CACHE
  READAHEAD_CACHE   WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  All
State:
  ONLINE to this controller
  Not reserved
  NOPREFERRED_PATH
Size:        17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
d2                                  DISK20000
LUN ID:        6000-1FE1-0000-01F0-0009-8490-6303-0135
NOIDENTIFIER
Switches:
  RUN                NOWRITE_PROTECT                READ_CACHE
  READAHEAD_CACHE   WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  All
State:
  ONLINE to this controller
  Not reserved
  NOPREFERRED_PATH
```

Size: 17769177 blocks
 Geometry (C/H/S): (5258 / 20 / 169)

- k. **Compaq OpenVMS only:** Use the following command to set each unit's device identifier to the value it was prior to hardware replacement:

```
SET UnitName IDENTIFIER = Value
Example: set d1 identifier = 1
```

This becomes the VMS device identifier for DGx1.

- ▶ 3. Disable all access to the units with the following CLI command:

```
SET UnitName DISABLE = ALL
Example: set d1 disable = all
```

Repeat this step for each unit.

- ▶ 4. Verify the disabled access with the following CLI command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 14.

Example Display 14

```
BuildngATop> show units full
LUN ----- Uses ----- Used by -----
D1                                     DISK10000
LUN ID:      6000-1FE1-0000-01F0-0009-8490-6303-0134
IDENTIFIER = 1
Switches:
  RUN                NOWRITE_PROTECT          READ_CACHE
  READAHEAD_CACHE    WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  None
State:
  ONLINE to this controller
  Not reserved
  NOPREFERRED_PATH
Size: 17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
D2                                     DISK20000
LUN ID:      6000-1FE1-0000-4250-0009-9411-5654-003F
NOIDENTIFIER
Switches:
  RUN                NOWRITE_PROTECT          READ_CACHE
  READAHEAD_CACHE    WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  None
State:
```

```

    ONLINE to this controller
    Not reserved
    NO PREFERRED_PATH
    Size:                17769177 blocks
    Geometry (C/H/S): ( 5258 / 20 / 169 )

```

- ▶ 5. At the initiator site, the units must be preferred to one controller or the other.
- a. Check for preference with the following CLI command. Use the same preference rules as used at the target:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 15.

Example Display 15

```

BuildngATop> show units full
D1                                     DISK10000
LUN ID:          6000-1FE1-0000-01F0-0009-8490-6303-0134
IDENTIFIER = 1
Switches:
  RUN                NOWRITE_PROTECT          READ_CACHE
  READAHEAD_CACHE    WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  None
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = THIS_CONTROLLER
Size:                17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
D2                                     DISK20000
LUN ID:          6000-1FE1-0000-01F0-0009-8490-6303-0135
NOIDENTIFIER
Switches:
  RUN                NOWRITE_PROTECT          READ_CACHE
  READAHEAD_CACHE    WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  None
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = OTHER_CONTROLLER
Size:                17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )

```

- b. If the units need to be preferred, use the following command:

```
SET UnitName PREFERRED_PATH = THIS_CONTROLLER
```

```
Example: set d1 preferred_path = this_controller
```

or

```
SET UnitName PREFERRED_PATH = OTHER_CONTROLLER
```

```
Example: set d2 preferred_path = other_controller
```

- ▶ 6. Set the maximum cached transfer size to 128 with the following CLI command:

```
SET UnitName MAXIMUM_CACHED_TRANSFER_SIZE = 128
```

```
Example: set d1 maximum_cached_transfer_size = 128
```

Repeat this step for each remote copy set unit.

NOTE: This command sets both the read and write maximum cached transfer size.

- ▶ 7. Enable Port 1 and Port 2 connections to the fabric with the following CLI commands:

```
SET THIS_CONTROLLER PORT_1_TOPOLOGY = FABRIC
```

```
SET OTHER_CONTROLLER PORT_1_TOPOLOGY = FABRIC
```

```
SET THIS_CONTROLLER PORT_2_TOPOLOGY = FABRIC
```

```
SET OTHER_CONTROLLER PORT_2_TOPOLOGY = FABRIC
```

- ▶ 8. Compare the status of the controllers, association sets, remote copy sets, units, and connections at the target site with those at the initiator site. A full procedure is detailed in Appendix A. Make sure any status change is reflected on the target. To compare status, bring up a terminal emulator session and enter the following commands.

```
SHOW THIS_CONTROLLER
```

```
SHOW OTHER_CONTROLLER
```

You will see a display similar to that in Example Display 16.

Example Display 16

```
BuildngATop> show this_controller
Controller:
  HSG80 ZG84906303 Software V86-1P, Hardware E03
  NODE_ID           = 5000-1FE1-0000-01F0
  ALLOCATION_CLASS   = 0
  SCSI_VERSION      = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG84906237
  In dual-redundant configuration
  Device Port SCSI address 7
  Time: 11-MAY-2001 12:04:30
```

```

Command Console LUN is lun 0 (IDENTIFIER = 99)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-01F3
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address          = 220213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-01F4
  PORT_2_TOPOLOGY = FABRIC (fabric up)
  Address          = 220413
  REMOTE_COPY     = BUILDNGA
Cache:
  256 megabyte write cache, version 0012
  Cache is GOOD
  No unflushed data in cache
  CACHE_FLUSH_TIMER = DEFAULT (10 seconds)
Mirrored Cache:
  256 megabyte write cache, version 0012
  Cache is GOOD
  No unflushed data in cache
Battery:
  NOUPS
  FULLY CHARGED
  Expires:          11-MAY-2003

BuildngATop> show other_controller
Controller:
  HSG80 ZG84906237 Software V86-1P, Hardware E03
  NODE_ID           = 5000-1FE1-0000-01F0
  ALLOCATION_CLASS   = 0
  SCSI_VERSION      = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG84906303
  In dual-redundant configuration
  Device Port SCSI address 6
  Time: 11-MAY-2001 12:08:17
  Command Console LUN is lun 0 (IDENTIFIER = 99)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-01F1
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address          = 250213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-01F2
  PORT_2_TOPOLOGY = FABRIC (fabric up)
  Address          = 250413
  REMOTE_COPY     = BUILDNGA
Cache:
  256 megabyte write cache, version 0012
  Cache is GOOD
  No unflushed data in cache
  CACHE_FLUSH_TIMER = DEFAULT (10 seconds)
Mirrored Cache:
  256 megabyte write cache, version 0012
  Cache is GOOD
  No unflushed data in cache
Battery:
  NOUPS
  FULLY CHARGED
  Expires:          11-MAY-2003

```

- ▶ 9. Continue the New Hardware Failback at the target site with the Target Site Preparation Procedure.

Target Site Preparation Procedure

This section describes how to prepare the target site for failback and create connections from the initiator site to the target.

1. Disable initiator controller access to all remote copy set units by issuing the following command:

```
SET UnitName DISABLE = InitiatorRemoteCopyNameA,
InitiatorRemoteCopyNameB, InitiatorRemoteCopyNameC,
InitiatorRemoteCopyNameD
```

Example: `set d1 disable = buildngAA,buildngAB,buildngAC,buildngAD`

Repeat this step for each remote copy set unit.

2. Verify the lack of controller access to the remote copy set with the following CLI command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 17.

Example Display 17

```
BuildngBTop> show units full
```

LUN	Uses	Used by
D1	DISK10000	BUILDNGA\RCS1
LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003E NOIDENTIFIER Switches: RUN NOWRITE_PROTECT READ_CACHE READAHEAD_CACHE WRITEBACK_CACHE MAX_READ_CACHED_TRANSFER_SIZE = 128 MAX_WRITE_CACHED_TRANSFER_SIZE = 128 Access: HOSTB1, HOSTB2 State: ONLINE to this controller Not reserved PREFERRED_PATH = THIS_CONTROLLER Target NORMAL Size: 17769177 blocks Geometry (C/H/S): (5258 / 20 / 169)		
D2	DISK20000	BUILDNGB\RCS2
LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003F NOIDENTIFIER Switches: RUN NOWRITE_PROTECT READ_CACHE READAHEAD_CACHE WRITEBACK_CACHE MAX_READ_CACHED_TRANSFER_SIZE = 128 MAX_WRITE_CACHED_TRANSFER_SIZE = 128 Access: HOSTB1, HOSTB2		


```
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = OTHER_CONTROLLER
Size:      17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
```

- 3. Delete the connections to the original controllers at the initiator site using the following CLI commands:

```
DELETE InitiatorRemoteCopyNameA
```

```
Example: delete buildngAA
```

```
DELETE InitiatorRemoteCopyNameB
```

```
Example: delete buildngAB
```

```
DELETE InitiatorRemoteCopyNameC
```

```
Example: delete buildngAC
```

```
DELETE InitiatorRemoteCopyNameD
```

```
Example: delete buildngAD
```

- 4. Verify the deletions with the following CLI command:

```
SHOW CONNECTIONS
```

You will see a display similar to that in Example Display 18.

Example Display 18

```
BuildngBTop> show connections
Connection
  Name      Operating system  Controller  Port  Address  Status  Unit
Offset
HOSTA1      WINNT             THIS        1     260013  OL this  0
HOST_ID=1000-0000-C920-A7B9  ADAPTER_ID=1000-0000-C920-A7B9
HOSTA2      WINNT             OTHER        1     200013  OL other  0
HOST_ID=1000-0000-C921-3F4E  ADAPTER_ID=1000-0000-C921-3F4E
HOSTB1      WINNT             THIS        1     220013  OL this  0
HOST_ID=1000-0000-C921-3E98  ADAPTER_ID=1000-0000-C921-3E98
HOSTB2      WINNT             OTHER        1     250013  OL other  0
HOST_ID=1000-0000-C921-3EFC  ADAPTER_ID=1000-0000-C921-3EFC
```

The only access to the target units will now be from the hosts.

- 5. To enable the connections to the initiator site, enter the following CLI commands:

```
SET THIS_CONTROLLER PORT_2_TOPOLOGY = FABRIC
```

```
SET OTHER_CONTROLLER PORT_2_TOPOLOGY = FABRIC
```

6. Verify that the connections were enabled with the following CLI commands:

```
SHOW THIS_CONTROLLER
SHOW OTHER_CONTROLLER
```

You will see a display similar to that in Example Display 19.

Example Display 19

```
BuildngBTop> show this_controller
Controller:
  HSG80 ZG94115654 Software V86-1P, Hardware E10
  NODE_ID = 5000-1FE1-0000-4250
  ALLOCATION_CLASS = 0
  SCSI_VERSION = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG94319198
    In dual-redundant configuration
  Device Port SCSI address 7
  Time: 11-MAY-2001 12:36:15
  Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-4253
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address = 260213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-4254
  PORT_2_TOPOLOGY = FABRIC (fabric up)
  Address = 260413
  REMOTE_COPY = BUILDNGB
.
.
.
BuildngBTop> show other_controller
Controller:
  HSG80 ZG94319198 Software V86-1P, Hardware E10
  NODE_ID = 5000-1FE1-0000-4250
  ALLOCATION_CLASS = 0
  SCSI_VERSION = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG94115654
    In dual-redundant configuration
  Device Port SCSI address 6
  Time: 10-MAY-2001 16:43:12
  Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-4251
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address = 200213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-4252
  PORT_2_TOPOLOGY = FABRIC (fabric up)
  REMOTE_COPY = BUILDNGB
.
.
.
```

IMPORTANT: Restore the intersite connections at this time.

- 7. Establish the connections to the initiator site with the following CLI command:

```
ADD REMOTE_COPY_SETS RCS199 D199 InitiatorRemoteCopyName\D199
```

Example: add remote_copy_sets rcs199 d199 buildngA\d199

NOTE: This command will report as failed with the error message: Error: Initiator Unit specified not found. However, it creates and names the connections appropriately.

- 8. Verify the connections with the following CLI command:

```
SHOW CONNECTIONS
```

You will see a display similar to that in Example Display 20.

Example Display 20

```
BuildngBTop> show connections
Connection
  Name      Operating system  Controller  Port  Address  Status  Unit
Offset
BUILDNGAA  PPRC_TARGET      THIS       2     offline  0
HOST_ID=5000-1FE1-0000-01F0  ADAPTER_ID=5000-1FE1-0000-01F4
BUILDNGAB  PPRC_TARGET      OTHER      2     offline  0
HOST_ID=5000-1FE1-0000-01F0  ADAPTER_ID=5000-1FE1-0000-01F2
BUILDNGAC  PPRC_INITIATOR   THIS       2     offline  0
HOST_ID=5000-1FE1-0000-01F0  ADAPTER_ID=5000-1FE1-0000-01F4
BUILDNGAD  PPRC_INITIATOR   OTHER      2     offline  0
HOST_ID=5000-1FE1-0000-01F0  ADAPTER_ID=5000-1FE1-0000-01F2
HOSTA1      WINNT            THIS       1     260013  OL this  0
HOST_ID=1000-0000-C920-A7B9  ADAPTER_ID=1000-0000-C920-A7B9
HOSTA2      WINNT            OTHER      1     200013  OL other 0
HOST_ID=1000-0000-C921-3F4E  ADAPTER_ID=1000-0000-C921-3F4E
HOSTB1      WINNT            THIS       1     220013  OL this  0
HOST_ID=1000-0000-C921-3E98  ADAPTER_ID=1000-0000-C921-3E98
HOSTB2      WINNT            OTHER      1     250013  OL other 0
HOST_ID=1000-0000-C921-3EFC  ADAPTER_ID=1000-0000-C921-3EFC
```

- 9. Continue the New Hardware Failback at the initiator site with the Initiator Site Connections Procedure.

Initiator Site Connections Procedure

This section describes how to create initiator site connections to the target.

- ▶ 1. Establish connection to the target site with the following CLI command:

```
ADD REMOTE_COPY_SETS RCS199 D199 TargetRemoteCopyName\D199
```

Example: `add remote_copy_sets rcs199 d199 buildngB\d199`

NOTE: This command will report as failed with the error message: `Error: Initiator Unit specified not found.` However, it creates and names the connections appropriately.

- ▶ 2. Verify the connections with the following CLI command:

```
SHOW CONNECTIONS
```

You will see a display similar to that in Example Display 21.

Example Display 21

```
BuildngABottom> show connections
Connection
Name          Operating system  Controller  Port  Address  Status  Unit
Offset
!NEWCON00     WINNT            OTHER       1     220013  OL other  0
HOST_ID=1000-0000-C921-3E98 ADAPTER_ID=1000-0000-C921-3E98
!NEWCON01     WINNT            OTHER       1     260013  OL other  0
HOST_ID=1000-0000-C920-A7B9 ADAPTER_ID=1000-0000-C920-A7B9
!NEWCON02     WINNT            THIS        1     250013  OL this   0
HOST_ID=1000-0000-C921-3EFC ADAPTER_ID=1000-0000-C921-3EFC
!NEWCON03     WINNT            THIS        1     200013  OL this   0
HOST_ID=1000-0000-C921-3F4E ADAPTER_ID=1000-0000-C921-3F4E
BUILDNGBA    PPRC_TARGET     OTHER       2           offline  0
HOST_ID=5000-1FE1-0000-4250 ADAPTER_ID=5000-1FE1-0000-4254
BUILDNGBB    PPRC_TARGET     THIS        2           offline  0
HOST_ID=5000-1FE1-0000-4250 ADAPTER_ID=5000-1FE1-0000-4252
BUILDNGBC    PPRC_INITIATOR  OTHER       2           offline  0
HOST_ID=5000-1FE1-0000-4250 ADAPTER_ID=5000-1FE1-0000-4254
BUILDNGBD    PPRC_INITIATOR  THIS        2           offline  0
HOST_ID=5000-1FE1-0000-4250 ADAPTER_ID=5000-1FE1-0000-4252
```

- ▶ 3. Enable target controller access to all remote copy set units by issuing the following CLI command:

```
SET UnitName ENABLE = TargetRemoteCopyNameA, TargetRemoteCopyNameB,
TargetRemoteCopyNameC, TargetRemoteCopyNameD
```

Example: set d1 enable = buildngBA, buildngBB, buildngBC, buildngBD

- ▶ 4. Verify the access with the following CLI command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 22.

Example Display 22

```
BuildngATop> show units full
      LUN                               Uses                Used by
-----
D1
LUN ID:          6000-1FE1-0000-01F0-0009-8490-6303-0134
IDENTIFIER = 1
Switches:
  RUN              NOWRITE_PROTECT          READ_CACHE
  READAHEAD_CACHE WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 128
  MAX_WRITE_CACHED_TRANSFER_SIZE = 128
Access:
  BUILDNGBA, BUILDNGBB, BUILDNGBC, BUILDNGBD
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = THIS_CONTROLLER
Size:          17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
D2
LUN ID:          6000-1FE1-0000-4250-0009-9411-5654-003F
NOIDENTIFIER
Switches:
  RUN              NOWRITE_PROTECT          READ_CACHE
  READAHEAD_CACHE WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 128
  MAX_WRITE_CACHED_TRANSFER_SIZE = 128
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = OTHER_CONTROLLER
Size:          17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
```

- ▶ 5. Continue the New Hardware Failback at the target site with the Target Site Copy Data Procedure.

Target Site Copy Data Procedure

The section describes how to copy the data from the target site to the initiator site.

1. Enable initiator controller access to all remote copy set units with this command:

```
SET UnitName ENABLE =
InitiatorRemoteCopyNameA, InitiatorRemoteCopyNameB,
InitiatorRemoteCopyNameC, InitiatorRemoteCopyNameD
```

Example: set d1 enable = buildngAA,buildngAB,buildngAC,buildngAD

2. Verify the access with the following CLI command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 23.

Example Display 23

```
BuildngATop> show units full
-----
```

LUN	Uses	Used by
D1	DISK10000	
LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0134		
IDENTIFIER = 1		
Switches:		
RUN	NOWRITE_PROTECT	READ_CACHE
READAHEAD_CACHE	WRITEBACK_CACHE	
MAX_READ_CACHED_TRANSFER_SIZE = 128		
MAX_WRITE_CACHED_TRANSFER_SIZE = 128		
Access:		
BUILDNGBA, BUILDNGBB, BUILDNGBC, BUILDNGBD, HOSTB1, HOSTB2		
State:		
ONLINE to this controller		
Not reserved		
PREFERRED_PATH = THIS_CONTROLLER		
Size: 17769177 blocks		
Geometry (C/H/S): (5258 / 20 / 169)		
D2	DISK20000	
LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003F		
NOIDENTIFIER		
Switches:		
RUN	NOWRITE_PROTECT	READ_CACHE
READAHEAD_CACHE	WRITEBACK_CACHE	
MAX_READ_CACHED_TRANSFER_SIZE = 128		
MAX_WRITE_CACHED_TRANSFER_SIZE = 128		
Access:		
BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD, HOSTB1, HOSTB2		
State:		
ONLINE to this controller		
Not reserved		
PREFERRED_PATH = OTHER_CONTROLLER		
Size: 17769177 blocks		
Geometry (C/H/S): (5258 / 20 / 169)		

- 3. Add back the target to the initiator unit's remote copy sets that were at the initiator site before failover with the following CLI command:

```
SET RemoteCopySetName ADD = InitiatorRemoteCopyName\UnitName
```

Example: set rcs1 add = buildngA\d1

You will see a confirmation message, as shown in Example Display 24.

Example Display 24

```
%EVL--BuildngBTop> --11-MAY-2001 12:53:20-- Instance Code: 0E050064
Template: 144.(90)
.
.
Instance Code: 0E050064
```

- 4. Verify that the initiator unit has been added back to the remote copy sets with the following CLI command:

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to that in Example Display 25.

Example Display 25

```
BuildngBTop> show remote_copy_sets full
Name                               Uses                               Used by
-----
RCS1          remote copy                D1
Reported LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003E
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGB\D1) state:
  ONLINE to this controller
  Not reserved
Target state:
  BUILDNGA\D1      is COPYING                1% complete
BuildngBTop> show remote_copy_sets full
Name                               Uses                               Used by
-----
RCS1          remote copy                D1
Reported LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003E
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGB\D1) state:
  ONLINE to this controller
  Not reserved
Target state:
  BUILDNGA\D1      is NORMAL
```

When the units are all normalized, the Target state field of the display will show NORMAL.

IMPORTANT: Wait for normalization on all remote copy sets to complete before proceeding.

- 5. If you plan to leave load running, you may now add write history logging to your association sets.

NOTE: For information on how to add write history logging to association sets, see Appendix C.

- 6. If you plan to leave load running, and your application requires failsafe mode, set failsafe mode with the following CLI command:

```
SET RemoteCopySetName ERROR_MODE = FAILSAFE
```

Example: set rcs1 error_mode = failsafe

Repeat this step for all applicable remote copy sets.

NOTE: Failsafe cannot be set if the remote copy set is in an association set that will be used for write history logging.

- 7. When you are ready to resume the failback process, continue with the following steps.

IMPORTANT: You must stop I/O from the target hosts to continue with the procedure from this point on.

- 8. Disable host access to all remote copy set units with the following CLI command:

```
SET UnitName DISABLE = TargetHostConnectionNamex,  
TargetHostConnectionNamey
```

Example: set d1 disable = hostb1,hostb2

- 9. Verify the disabled host access with the following CLI command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 26.

Example Display 26

```
BuildngBTop> show units full
LUN                               Uses                               Used by
-----
D1                                  DISK10000                          BUILDNGB\RCS1
LUN ID:          6000-1FE1-0000-4250-0009-9411-5654-003E
NOIDENTIFIER
Switches:
  RUN              NOWRITE_PROTECT              READ_CACHE
  READAHEAD_CACHE WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
```



```

MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = THIS_CONTROLLER
Size:      17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
D2
                                DISK20000
LUN ID:      6000-1FE1-0000-4250-0009-9411-5654-003F
NOIDENTIFIER
Switches:
  RUN                NOWRITE_PROTECT                READ_CACHE
  READAHEAD_CACHE   WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 128
  MAX_WRITE_CACHED_TRANSFER_SIZE = 128
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = OTHER_CONTROLLER
Size:      17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )

```

- ⑩ 10. Continue the New Hardware Failback at the initiator site with the Initiator Site Return Control Procedure.

Initiator Site Return Control Procedure

This section describes how to return Data Replication Manager control to the initiator site.

- ▶ 1. Disconnect controller access with the following CLI command:

```

SET THIS_CONTROLLER PORT_2_TOPOLOGY = OFFLINE
SET OTHER_CONTROLLER PORT_2_TOPOLOGY = OFFLINE

```

- ▶ 2. Verify the disconnection with the following CLI commands:

```

SHOW THIS_CONTROLLER
SHOW OTHER_CONTROLLER

```

You will see a display similar to that in Example Display 27.

Example Display 27

```

BuildngATop> show this_controller
Controller:
  HSG80 ZG84906303 Software V86-1P, Hardware E03
  NODE_ID           = 5000-1FE1-0000-01F0
  ALLOCATION_CLASS   = 0
  SCSI_VERSION      = SCSI-3

```

```
Configured for MULTIBUS_FAILOVER with ZG84906237
  In dual-redundant configuration
Device Port SCSI address 7
Time: 11-MAY-2001 13:33:31
Command Console LUN is lun 0 (IDENTIFIER = 99)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-01F3
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address          = 220213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-01F4
  PORT_2_TOPOLOGY = OFFLINE (offline)
  REMOTE_COPY = BUILDNGA
.
.
.
BuildngBTop> show other_controller
Controller:
  HSG80 ZG84906237 Software V86-1P, Hardware E03
  NODE_ID          = 5000-1FE1-0000-01F0
  ALLOCATION_CLASS = 0
  SCSI_VERSION     = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG84906303
  In dual-redundant configuration
  Device Port SCSI address 6
  Time: 11-MAY-2001 12:08:17
  Command Console LUN is lun 0 (IDENTIFIER = 99)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-01F1
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address          = 250213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-01F2
  PORT_2_TOPOLOGY = OFFLINE (offline)
  Address          = 250413
  REMOTE_COPY = BUILDNGA
.
.
.
```

- ▶ 3. Move the initiator role to the original initiator with the following CLI command:

```
SITE_FAILOVER TargetRemoteCopyName\RemoteCopySetName
```

Example: `site_failover buildngB\rcs1`

You will see a confirmation message, as shown in Example Display 28.

Example Display 28

```
%EVL--BuildngATop> --10-MAY-2001 17:57:17-- Instance Code: 0E010064
Template: 144.(90)
Occurred on 10-MAY-2001 at 17:57:17
Power On Time: 2. Years, 45. Days, 10. Hours, 44. Minutes, 43. Seconds
Controller Model: HSG80
Serial Number: ZG84906303 Hardware Version: E03(2B)
Software Version: V86-1P
Informational Report
```

```

Target Controller Board Serial Number: "          ....."
Initiator WWLID: 6000-1FE1-0000-01F0-0009-8490-6303-0134
Initiator Node Name: "BUILDNGA"
Initiator Unit Number: 1.(00000001)
Target WWLID: 6000-1FE1-0000-4250-0009-9411-5654-003E
Target Node Name: "BUILDNGB"
Target Unit Number: 1.(00000001)
Number of Targets: 1.(00000001)
Remote Copy Set Name: "RCS1"
Association Set Name: ""
Log Unit Number: Not Available
Instance Code: 0E010064
    
```

- ▶ 4. Verify the initiator site setup with the following CLI command:

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to that in Example Display 29.

Example Display 29

```

BuildngATop> show remote_copy_sets full
Name                               Uses                               Used by
-----
RCS1                                remote copy                        D1
Reported LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003E
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGA\D1) state:
  ONLINE to this controller
  Not reserved
Target state:
BUILDNGB\D1      is COPYING                               1% complete
BuildngATop> show remote_copy_sets full
Name                               Uses                               Used by
-----
RCS1                                remote copy                        D1
Reported LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003E
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGA\D1) state:
  ONLINE to this controller
  Not reserved
Target state:
BUILDNGB\D1      is NORMAL
    
```

NOTE: Verify that the initiator is identified as BUILDNGA and the target is identified as BUILDNGB.

- ▶ 5. Continue the New Hardware Failback at the target site with the Target Site Restore Procedure.

Target Site Restore Procedure

1. Turn off write history logging, if enabled, with the following CLI command:

```
SET AssociationSetName NOLOG_UNIT
```

Example: `set as_d1 nolog_unit`

Repeat this step for each applicable association set.

2. Verify that write history logging has been turned off with the following CLI command:

```
SHOW ASSOCIATIONS FULL
```

You will see a display similar to that in Example Display 30.

Example Display 30

```
BuildngBTop> show associations full
Name          Association          Uses          Used by
-----
AS_D1         association          RCS1
                                   RCS2

Switches:
NOFAIL_ALL
NOORDER_ALL
NOLOG_UNIT
```

Repeat this procedure for each association set.

3. Delete the association set by using the following CLI command:

```
DELETE AssociationSetName
```

Example: `delete as_d1`

4. Delete all remote copy sets with the following CLI command:

```
DELETE RemoteCopySetName
```

Example: `delete rcs1`

Repeat this step for each remote copy set.

5. Set the maximum cached transfer size to 128 with the following CLI command:

```
SET UnitName MAXIMUM_CACHED_TRANSFER_SIZE = 128
```

Example: `set d1 maximum_cached_transfer_size = 128`

Repeat this step for each remote copy set.

- 6. After completing the above action, verify the maximum cached transfer size with the following CLI command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 31.

Example Display 31

```
BuildngBTop> show units full
-----
LUN                               Uses                               Used by
-----
D1                                DISK10000
LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003E
NOIDENTIFIER
Switches:
  RUN                               NOWRITE_PROTECT                   READ_CACHE
  READAHEAD_CACHE                   WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 128
  MAX_WRITE_CACHED_TRANSFER_SIZE = 128
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = THIS_CONTROLLER
Size: 17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )

D2                                DISK20000
LUN ID: 6000-1FE1-0000-4250-0009-9411-5654-003F
NOIDENTIFIER
Switches:
  RUN                               NOWRITE_PROTECT                   READ_CACHE
  READAHEAD_CACHE                   WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 128
  MAX_WRITE_CACHED_TRANSFER_SIZE = 128
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = OTHER_CONTROLLER
Size: 17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
```

NOTE: This command sets both the read and write maximum cached transfer size.

- 7. Continue the New Hardware Failback at the initiator site with the Initiator Site Restoration of Target Connections Procedure.

Initiator Site Restoration of Target Connections Procedure

This section describes how to restore all target connections from the initiator site.

- ▶ 1. To restore the connections to the target site, enter the following CLI commands:

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

- ▶ 2. Verify the restoration with the following CLI command:

```
SHOW THIS_CONTROLLER
SHOW OTHER_CONTROLLER
```

You will see a display similar to that in Example Display 32.

Example Display 32

```
BuildngATop> show this_controller
Controller:
  HSG80 ZG84906303 Software V86-1P, Hardware E03
  NODE_ID = 5000-1FE1-0000-01F0
  ALLOCATION_CLASS = 0
  SCSI_VERSION = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG84906237
    In dual-redundant configuration
  Device Port SCSI address 7
  Time: 11-MAY-2001 13:43:37
  Command Console LUN is lun 0 (IDENTIFIER = 99)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-01F3
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address = 220213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-01F4
  PORT_2_TOPOLOGY = FABRIC (fabric up)
  Address = 220413
  REMOTE_COPY = BUILDNGA
.
.
.
BuildngBTop> show other_controller
Controller:
  HSG80 ZG84906237 Software V86-1P, Hardware E03
  NODE_ID = 5000-1FE1-0000-01F0
  ALLOCATION_CLASS = 0
  SCSI_VERSION = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG84906303
    In dual-redundant configuration
  Device Port SCSI address 6
  Time: 11-MAY-2001 12:08:17
  Command Console LUN is lun 0 (IDENTIFIER = 99)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-01F1
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address = 250213
```

```
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-01F2
  PORT_2_TOPOLOGY = FABRIC (fabric up)
  Address          = 250413
  REMOTE_COPY     = BUILDNGA
  .
  .
  .
```

- ▶ 3. If you decide to, you can now change remote copy sets to asynchronous mode with the following CLI command:

```
SET RemoteCopySetName OPERATION_MODE = ASYNCHRONOUS
```

Example: `set rcs1 operation_mode = asynchronous`

Repeat this step for all applicable remote copy sets.

- ▶ 4. Create association sets and then add the log unit, if desired. For information on how to create association sets, with or without write history logging, see Appendix C.

IMPORTANT: If you will be using scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention (remote copy sets, stripesets, mirrorsets, RAIDsets, association sets, and connections)—use underscores instead. Dashes are not allowed by the Perl scripting language.

- ▶ 5. Verify the creation with the following CLI command:

```
SHOW ASSOCIATIONS FULL
```

You will see a display similar to that in Example Display 33.

Example Display 33

```
BuildngATop> show associations full
Name          Association          Uses          Used by
-----
AS_D1         association          RCS1
              RCS2

Switches:
NOFAIL_ALL
NOORDER_ALL
LOG_UNIT = D10 (No data logged)
```

- ▶ 6. Re-enable failsafe mode, if desired. To set failsafe mode, enter the following CLI command:

```
SET RemoteCopySetName ERROR_MODE = FAILSAFE
```

Example: `set rcs1 error_mode = failsafe`

NOTE: Failsafe cannot be set if the remote copy set is in an association set that will be used for write history logging.

- ▶ 7. If the initiator hosts were shut down, reboot them now. Rename all !NEWCONxx connections to their previous names with the following CLI command:

```
RENAME !NEWCONxx InitiatorHostConnectionName
```

Example: rename !newconxx hostA1

- ▶ 8. Verify the connections with the following CLI command:

```
SHOW CONNECTIONS
```

You will see a display similar to that in Example Display 34.

Example Display 34

```
BuildngATop> show connections
Connection
  Name      Operating system  Controller  Port  Address  Status  Unit
Offset
BUILDNGBA  PPRC_TARGET      THIS        2     260413  OL this  0
HOST_ID=5000-1FE1-0000-4250 ADAPTER_ID=5000-1FE1-0000-4254
BUILDNGBB  PPRC_TARGET      OTHER       2     200413  OL other  0
HOST_ID=5000-1FE1-0000-4250 ADAPTER_ID=5000-1FE1-0000-4252
BUILDNGBC  PPRC_INITIATOR   THIS        2                offline  0
HOST_ID=5000-1FE1-0000-4250 ADAPTER_ID=5000-1FE1-0000-4254
BUILDNGBD  PPRC_INITIATOR   OTHER       2                offline  0
HOST_ID=5000-1FE1-0000-4250 ADAPTER_ID=5000-1FE1-0000-4252
HOSTA1    WINNT          THIS        1     260013  OL this  0
HOST_ID=1000-0000-C920-A7B9 ADAPTER_ID=1000-0000-C920-A7B9
HOSTA2    WINNT          OTHER       1     200013  OL other  0
HOST_ID=1000-0000-C921-3F4E ADAPTER_ID=1000-0000-C921-3F4E
HOSTB1    WINNT          THIS        1     220013  OL this  0
HOST_ID=1000-0000-C921-3E98 ADAPTER_ID=1000-0000-C921-3E98
HOSTB2    WINNT          OTHER       1     250013  OL other  0
HOST_ID=1000-0000-C921-3EFC ADAPTER_ID=1000-0000-C921-3EFC
```

- ▶ 9. Set all connections that were renamed back to their appropriate operating system with the following CLI command.

```
SET InitiatorHostConnectionName OPERATING_SYSTEM = (HP, IBM,
NETWARE, SUN, Compaq Tru64_UNIX, VMS, or WINNT)
```

Example: set hostA1 operating_system = vms

- ▶ 10. Verify the connections with the following CLI command:

```
SHOW CONNECTIONS
```


You will see a display similar to that in Example Display 35.

Example Display 35

```
BuildngATop> show connections
Connection
Name      Operating system  Controller  Port   Address  Status  Unit
Offset
BUILDNGBA  PPRC_TARGET      THIS        2      260413  OL this  0
HOST_ID=5000-1FE1-0000-4250 ADAPTER_ID=5000-1FE1-0000-4254
BUILDNGBB  PPRC_TARGET      OTHER       2      200413  OL other  0
HOST_ID=5000-1FE1-0000-4250 ADAPTER_ID=5000-1FE1-0000-4252
BUILDNGBC  PPRC_INITIATOR   THIS        2      offline  0
HOST_ID=5000-1FE1-0000-4250 ADAPTER_ID=5000-1FE1-0000-4254
BUILDNGBD  PPRC_INITIATOR   OTHER       2      offline  0
HOST_ID=5000-1FE1-0000-4250 ADAPTER_ID=5000-1FE1-0000-4252
HOSTA1    VMS            THIS        1      260013  OL this  0
HOST_ID=1000-0000-C920-A7B9 ADAPTER_ID=1000-0000-C920-A7B9
HOSTA2    VMS            OTHER       1      200013  OL other  0
HOST_ID=1000-0000-C921-3F4E ADAPTER_ID=1000-0000-C921-3F4E
HOSTB1    VMS            THIS        1      220013  OL this  0
HOST_ID=1000-0000-C921-3E98 ADAPTER_ID=1000-0000-C921-3E98
HOSTB2    VMS            OTHER       1      250013  OL other  0
HOST_ID=1000-0000-C921-3EFC ADAPTER_ID=1000-0000-C921-3EFC
```

- ▶ 11. You can enhance host I/O performance by resetting the maximum cached transfer size to the value used on the original initiator. Obtain your record of `SHOW` command output that details the original initiator configuration. Using the output as a reference, set the maximum cached transfer size to the original initiator value using the following CLI command:

```
SET UnitName MAXIMUM_CACHED_TRANSFER_SIZE = InitiatorValue
```

```
Example: set d1 maximum_cache_transfer_size = 32
```

Repeat this step for all remote copy set units.

NOTE: The default maximum cache transfer size is 32.

- ▶ 12. Enable host access to the units by using the following CLI command:

```
SET UnitName ENABLE = InitiatorHostConnectionNamex,  
InitiatorHostConnectionNamey
```

```
Example: set d1 enable = hosta1, hosta2
```

- ▶ 13. Verify host access with the following CLI command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 36.

Repeat this step for all units.

Example Display 36

```

BuildingATop> show units full
-----
LUN                               Uses                               Used by
-----
D1                                  DISK10000                          BUILDNGA\RCS1
LUN ID:        6000-1FE1-0000-01F0-0009-8490-6303-0134
IDENTIFIER = 1
Switches:
  RUN          NOWRITE_PROTECT      READ_CACHE
  READAHEAD_CACHE  WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  BUILDNGBA, BUILDNGBB, BUILDNGBC, BUILDNGBD,  HOSTA1,  HOSTA2
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = THIS_CONTROLLER
Size:          17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )

D2                                  DISK20000
LUN ID:        6000-1FE1-0000-01F0-0009-8490-6303-0135
NOIDENTIFIER
Switches:
  RUN          NOWRITE_PROTECT      READ_CACHE
  READAHEAD_CACHE  WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  BUILDNGBA, BUILDNGBB, BUILDNGBC, BUILDNGBD,  HOSTA1,  HOSTA2
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = OTHER_CONTROLLER
Size:          17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
  
```

- ▶ 14. Allow hosts to recognize new units. Follow the steps listed below for each operating system in your heterogeneous configuration:
 - a. **Compaq OpenVMS:** If the initiator site hosts are shut down, boot them now. Booting the hosts enables OpenVMS to recognize the drives.

If the initiator site hosts are not shut down, use the following command from a privileged account to enable OpenVMS to recognize the drives:

MCR SYSMAN IO AUTOCONFIGURE/LOG
 - b. **Compaq Tru64 UNIX:** If the initiator site hosts are shut down, boot them now. Booting the hosts enables Tru64 UNIX to recognize the drives.

If the initiator site hosts are not shut down, use the following command to recognize the drives:

```
hwmgr - scan scsi
```

This might take a while for large configurations. If this is the case, scan only those SCSI buses that have new units added. Scan only one bus at a time. Use the following command:

```
hwmgr -scan scsi -bus x
```

where x is the SCSI bus number.

- c. **HP-UX:** If the initiator site hosts are shut down, boot them now. Booting the hosts enables HP-UX to recognize the drives.

If the initiator site hosts are not shut down, use the following commands to recognize the drives and mount the file systems:

```
ioscan -fnCdisk
```

```
mount -a
```

- d. **IBM AIX:** If the initiator site hosts are shut down, boot them now. Booting the hosts enables IBM AIX to recognize the drives.

If the initiator site hosts are not shut down, use the following commands to recognize the drives and mount the file systems:

```
cfgmgr -v
```

```
mount all
```

- e. **Microsoft Windows NT-X86:** Reboot the hosts at the initiator site and log in using an account that has administrative privileges. You should be able to see all of the units by choosing **My Computer**.

- f. **Microsoft Windows 2000:**

- 1) If you *have not* changed the UNIT_OFFSET of any host connections since the hosts have been booted, you do not need to reboot the initiator site hosts.

- a) On each host, log in using an account that has administrative privileges.

- b) Open **Computer Management** and click **Disk Management**.

- c) After **Disk Management** has initialized, go to the **Action** menu and click **Rescan Disks**. All of the failed over units should appear in the right-hand pane. If Secure Path is not installed correctly, you will see each unit twice.

2) If you *have* changed the UNIT_OFFSET of any host connections, you must reboot that host. After the server has rebooted, log in using an account that has administrative privileges. You will see all of the units in **Computer Management > Disk Management**. If Secure Path is not installed correctly, you will see each drive twice.

- g. **Novell NetWare:** If the initiator site hosts are shut down, boot them now. Booting the hosts allows Novell NetWare to recognize the drives.

If the initiator site hosts are already up and running, or if they do not recognize the drives, issue the following command from the console before mounting the volumes:

```
SCAN FOR NEW DEVICES
```

Alternatively, you can use the `NWCONFIG` utility to issue this same command.

- h. **SUN Solaris:** Reboot the hosts using the command `reboot -- -r` at the initiator site and log in using an account that has administrative privileges. You should be able to see all of the units by using the `format` command.

If Secure Path was not configured for these units, you will not see the drives. You will need to edit the WWLIDs in the file `/kernel/drv/ldLite.conf`. To find the new WWLIDs of the units, use the `SHOW Unitname` command on the controller. You may also need to adjust the files `/kernel/drv/mda.conf` and `/kernel/drv/sd.conf` to accommodate the extras LUNs. When you have edited `ldLite.conf`, `mda.conf`, and `sd.conf`, reboot the host using the `reboot -- -r` command. You should now be able to see the drives using the `format` command. Refer to the *Compaq SANworks Secure Path for Sun Solaris Installation and Reference Guide* for additional assistance.

This completes the Unplanned Site Failover with Failback to New Hardware.

Planned Site Role Reversal Procedure

In this situation you will be performing a planned move of initiator operations from the initiator site to an alternate (target) site. You will prepare the initiator site for the failover, then perform a failover to the alternate site. The original initiator site remains intact, operational, and online during the role reversal. You will then perform a role reversal failback to the original initiator site, when desired.

This chapter contains the following procedures to ensure that failover and subsequent failback during a role reversal scenario function properly:

- “Role Reversal Failover” on page 10–1
- “Role Reversal Failback” on page 10–17

NOTE: In this chapter, *initiator* site procedure steps are identified by an arrow symbol ► in the margin. *Target* site procedure steps are identified by a target symbol ⊙ in the margin.

NOTE: Some example displays illustrate confirmation messages with the event log symbol (%EVL) and an instance code. Compare the instance code in the example with the instance code you receive. If the numbers are the same, you have performed the previous command correctly and have achieved the desired results. Note that you will be able to see these screens only if you are working from the controller to which the LUNs are online. Refer to the Troubleshooting chapter for more information on instance codes and their meanings.

Example displays may also contain bold text to identify information that is the most pertinent in the example. In many cases, items shown in bold text will help you verify the results of a previous command.

Role Reversal Failover

To carry out a Role Reversal Failover, follow the procedure outlined in the following sections, in conjunction with the Role Reversal Failback. The Role Reversal Failover consists of the following procedures:

- Initiator Site Preparation Procedure
- Target Site Failover Procedure
- Target Host Setup Procedure

Initiator Site Preparation Procedure

- ▶ 1. Before performing the failover procedure, locate your record of `SHOW` command output that details the current initiator configuration.

Verify that your target controller configuration is the same as your initiator controller configuration. Compare the status of the controllers, association sets, remote copy sets, units, and connections. Appendix A contains the full procedure.

- ▶ 2. Verify that all remote copy sets are in the normal state by issuing the following command:

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to that in Example Display 1.

Example Display 1

```
BuildngATop> SHOW REMOTE_COPY_SETS FULL
Name                               Uses           Used by
-----
RCS1      remote copy                D1           AS_D1
Reported LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0134
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGA\D1) state:
  ONLINE to this controller
  Not reserved
Target state:
  BUILDNGB\D1      is NORMAL

RCS2      remote copy                D2
Reported LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0135
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 20
Initiator (BUILDNGA\D2) state:
  ONLINE to this controller
  Not reserved
Target state:
  BUILDNGB\D2      is NORMAL
```

- ▶ 3. Follow the steps listed below for each operating system in your heterogeneous configuration:
- a. **Compaq OpenVMS:** If the operating system is up and running, and is being used exclusively for DRM operations, shut down the operating system and power off the hosts. If the operating system is being used for other applications, remove all I/O to the remote copy set LUNs that will be failed over, then dismount the volumes associated with these LUNs.
 - b. **Compaq Tru64 UNIX:** If the operating system is up and running and is being used exclusively for DRM operations, shut down the operating system and power off the hosts. If the operating system is being used for other applications, remove all I/O and unmount all file system LUNs that have remote copy sets that will be failed over.
 - c. **HP-UX:** If the operating system is up and running, remove all I/O to the remote copy set LUNs that will be failed over, then unmount the file systems associated with these LUNs.
 - d. **IBM AIX:** If the operating system is up and running, remove all I/O to the remote copy set LUNs that will be failed over, then unmount the file systems associated with these LUNs.
 - e. **Microsoft Windows NT-X86:** If the operating system is up and running, shut it down and power off the hosts.
 - f. **Microsoft Windows 2000:** If the operating system is up and running, shut it down and power off the hosts.
 - g. **Novell NetWare:** If the operating system is up and running, remove all I/O to the remote copy set LUNs that will be failed over, then dismount the volumes associated with these LUNs.

If you are using NetWare Cluster Services (NWCS), you must enter the `cluster down` command. You must also enter the `uldncs` (unload NetWare Cluster Services) command for all cluster nodes.



CAUTION: Failure to enter these two commands will cause all cluster nodes to abend.

- h. **SUN Solaris:** If the operating system is up and running and is being used exclusively for DRM operations, shut down the operating system and power off the hosts. If the operating system is being used for other applications, remove all I/O and unmount all volumes that have remote copy sets that will be failed over.

- ▶ 4. If your remote copy sets are set for asynchronous operation mode, switch to synchronous mode using the following CLI command:

```
SET RemoteCopySetName OPERATION_MODE = SYNCHRONOUS
```

Example: set rcs1 operation_mode = synchronous

Repeat this step for all applicable remote copy sets.

- ▶ 5. Turn off write history logging, if enabled, with the following CLI command:

```
SET AssociationSetName NOLOG_UNIT
```

Example: set as_d1 nolog_unit

Repeat this procedure for each association set.

- ▶ 6. Delete any association sets with the following CLI command:

```
DELETE AssociationSetName
```

Example: delete as_d1

Repeat this procedure for each association set.

- ▶ 7. Disable host access to the remote copy set units with the following CLI command:

NOTE: Do not disable access to the target connection.

```
SET UnitName DISABLE = InitiatorHostConnectionNamex,  
InitiatorHostConnectionNamey
```

Example: set d1 disable = hosta1,hosta2

Repeat this step for all remote copy set units.

- ▶ 8. Each remote copy set unit should have four connections enabled to TargetRemoteCopyNameA, TargetRemoteCopyNameB, TargetRemoteCopyNameC, and TargetRemoteCopyNameD.

- a. Verify the access path for each unit used by remote copy sets by entering the following CLI command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 2.

Example Display 2

```

BuildngATop> SHOW UNITS FULL
LUN                               Uses                               Used by
-----
D1                                  DISK10000                          BUILDNGA\RCS1
LUN ID:                            6000-1FE1-0000-01F0-0009-8490-6303-0134
NOIDENTIFIER
Switches:
  RUN                               NOWRITE_PROTECT                     READ_CACHE
  READAHEAD_CACHE                   WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  BUILDNGBA, BUILDNGBB, BUILDNGBC, BUILDNGBD
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = THIS_CONTROLLER
Size:                               17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )

D2                                  DISK20000                          BUILDNGA\RCS2
LUN ID:                            6000-1FE1-0000-01F0-0009-8490-6303-0134
NOIDENTIFIER
Switches:
  RUN                               NOWRITE_PROTECT                     READ_CACHE
  READAHEAD_CACHE                   WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  BUILDNGBA, BUILDNGBB, BUILDNGBC, BUILDNGBD
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = OTHER_CONTROLLER
Size:                               17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )

```

- b. If target controller access to the units used by remote copy sets is not currently enabled, enable access by issuing the following command for each unit:

```

SET UnitName ENABLE = TargetRemoteCopyNameA,
TargetRemoteCopyNameB, TargetRemoteCopyNameC,
TargetRemoteCopyNameD

```

Example: set d1 enable = buildngbA,buildngbB,buildngbC, buildngbD

9. Set maximum cached transfer size for all remote copy set units to 128 with the following CLI command:

```

SET UnitName MAXIMUM_CACHED_TRANSFER_SIZE = 128

```

Example: set d1 maximum_cached_transfer_size = 128

Repeat this step for all remote copy set units.

NOTE: This command sets both the read and write maximum cached transfer size.

- ▶ 10. Continue the Role Reversal Failover process at the target site with the Target Site Failover Procedure.

Target Site Failover Procedure

- ◎ 1. At the target site, the units must be preferred to one controller or the other.
 - a. Use the following CLI command to check for the preferred path:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 3.

Example Display 3

```
BuildngBTop> SHOW UNITS FULL
-----
LUN                               Uses                               Used by
-----
D1                                  DISK10000                          BUILDNGA\RCS1
LUN ID:          6000-1FE1-0000-4250-0009-9411-5654-003E
NOIDENTIFIER
Switches:
  RUN              NOWRITE_PROTECT          READ_CACHE
  READAHEAD_CACHE  WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 128
  MAX_WRITE_CACHED_TRANSFER_SIZE = 128
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = THIS_CONTROLLER
  Target NORMAL
Size:              17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
D2                                  DISK20000                          BUILDNGA\RCS2
LUN ID:          6000-1FE1-0000-4250-0009-9411-5654-003F
NOIDENTIFIER
Switches:
  RUN              NOWRITE_PROTECT          READ_CACHE
  READAHEAD_CACHE  WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 128
  MAX_WRITE_CACHED_TRANSFER_SIZE = 128
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = OTHER_CONTROLLER
  Target NORMAL
Size:              17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
```

- b. If units are not currently preferred, use the following CLI command:

```
SET UnitName PREFERRED_PATH = THIS_CONTROLLER
```

```
Example: set d1 preferred_path = this_controller
```

or

```
SET UnitName PREFERRED_PATH = OTHER_CONTROLLER
```

```
Example: set d2 preferred_path = other_controller
```

Repeat this step for each remote copy set unit that needs to be preferred.

2. Disconnect controller access with the following CLI commands:

```
SET THIS_CONTROLLER PORT_2_TOPOLOGY = OFFLINE
```

```
SET OTHER_CONTROLLER PORT_2_TOPOLOGY = OFFLINE
```

3. Verify the disconnect by performing the following CLI commands:

```
SHOW THIS_CONTROLLER
```

```
SHOW OTHER_CONTROLLER
```

You will see a display similar to that in Example Display 4.

Example Display 4

```
BuildngBTop> show this_controller
Controller:
  HSG80 ZG84906303 Software V86-1P, Hardware E03
  NODE_ID           = 5000-1FE1-0000-01F0
  ALLOCATION_CLASS   = 0
  SCSI_VERSION      = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG84906237
  In dual-redundant configuration
  Device Port SCSI address 7
  Time: 10-MAY-2001 17:55:29
  Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-01F3
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address          = 220213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-01F4
  PORT_2_TOPOLOGY = OFFLINE (offline)
  REMOTE_COPY = BUILDNGA
.
.
.
BuildngBTop> show other_controller
Controller:
  HSG80 ZG84906237 Software V86-1P, Hardware E03
  NODE_ID           = 5000-1FE1-0000-01F0
  ALLOCATION_CLASS   = 0
  SCSI_VERSION      = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG84906303
  In dual-redundant configuration
  Device Port SCSI address 6
```

```
Time: 10-MAY-2001 17:55:39
Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-01F1
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address          = 250213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-01F2
  PORT_2_TOPOLOGY = OFFLINE (offline)
  REMOTE_COPY     = BUILDNGA
.
.
.
```

4. Move the initiator role to the target site with the following CLI command:

```
SITE_FAILOVER InitiatorRemoteCopyName\RemoteCopySetName
```

Example: `site_failover buildnga\rsc1`

You will see a confirmation message, as shown in Example Display 5.

Example Display 5

```
BuildngBTop> site_failover Buildnga\rsc1
%EVL--BuildngBTop> --10-MAY-2001 15:47:39-- Instance Code: 0E010064
Template: 144.(90)
.
.
.
Instance Code: 0E010064
```

Repeat this step for each remote copy set.

5. Restore the connections to the target site with the following CLI commands:

```
SET THIS_CONTROLLER PORT_2_TOPOLOGY = FABRIC
```

```
SET OTHER_CONTROLLER PORT_2_TOPOLOGY = FABRIC
```

6. After completing this action, verify the restoration with the following CLI commands.

```
SHOW THIS_CONTROLLER
```

```
SHOW OTHER_CONTROLLER
```

You will see a display similar to that in Example Display 6.

Example Display 6

```

BuildngBTop> show this_controller
Controller:
  HSG80 ZG94115654 Software V86-1P, Hardware E10
  NODE_ID           = 5000-1FE1-0000-4250
  ALLOCATION_CLASS   = 0
  SCSI_VERSION      = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG94319198
  In dual-redundant configuration
  Device Port SCSI address 7
  Time: 10-MAY-2001 17:34:11
  Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-4253
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address          = 260213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-4254
  PORT_2_TOPOLOGY = FABRIC (fabric up)
  Address          = 260413
  REMOTE_COPY     = BUILDNGB
.
.
.
BuildngBTop> show other_controller
Controller:
  HSG80 ZG94319198 Software V86-1P, Hardware E10
  NODE_ID           = 5000-1FE1-0000-4250
  ALLOCATION_CLASS   = 0
  SCSI_VERSION      = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG94115654
  In dual-redundant configuration
  Device Port SCSI address 6
  Time: 10-MAY-2001 17:34:20
  Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-4251
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address          = 200213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-4252
  PORT_2_TOPOLOGY = FABRIC (fabric up)
  Address          = 200413
  REMOTE_COPY     = BUILDNGB
.
.
.

```

- ⑦ 7. If you changed an asynchronous remote copy set to synchronous during failover, change it back to asynchronous mode by issuing the following CLI command:

```
SET RemoteCopySetName OPERATION_MODE = ASYNCHRONOUS
```

Example: set rcs1 operation_mode = asynchronous

Repeat this step for all applicable remote copy sets.

- 8. If desired, create association sets and set up write history logging to duplicate the association sets that are on the initiator.

Repeat this step for each applicable association set.

IMPORTANT: If you will be using scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention (remote copy sets, stripesets, mirrorsets, RAIDsets, association sets, and connections)—use underscores instead. Dashes are not allowed by the Perl scripting language.

NOTE: The procedure to create association sets is contained in Appendix C.

- 9. When you have created the association sets, verify the creation with the following CLI command:

```
SHOW ASSOCIATIONS FULL
```

You will see a display similar to Example Display 7.

Example Display 7

```
BuildngBTop> show associations full
Name          Association          Uses          Used by
-----
AS_D1         association          RCS1
    Switches:
    NOFAIL_ALL
    NOORDER_ALL
    LOG_UNIT = D10 (99% available)
```

- 10. Re-enable failsafe mode, if desired. To set failsafe mode, enter the following CLI command:

```
SET RemoteCopySetName ERROR_MODE = FAILSAFE
```

Example: `set rcs1 error_mode = failsafe`

Repeat this step for all applicable remote copy sets.

NOTE: Failsafe cannot be set if the remote copy set is in an association set that will be used for write history logging.

- 11. Continue the failover procedure at the target site with the Target Host Setup Procedure.

Target Host Setup Procedure

1. If you wish, you can enhance host I/O performance by resetting the maximum cached transfer size to the value used on the initiator. Use this command:

```
SET UnitName MAXIMUM_CACHED_TRANSFER_SIZE = InitiatorValue
```

```
Example: set d1 maximum_cached_transfer_size = 32
```

Repeat this step for each unit.

NOTE: The default maximum cached transfer size is 32.

2. Give the target site hosts access to the units that are used by remote copy sets in the storage subsystems with this command:

```
SET UnitName ENABLE = TargetHostConnectionNamex,  
TargetHostConnectionNamey
```

```
Example: set d1 enable = hostb1,hostb2
```

You will see a display similar to that in Example Display 8.

Example Display 8

```
BuildngBTop> set d1 enable=hostb1,hostb2  
Warning 1000: Other host(s) in addition to the one(s) specified can still  
access this unit. If you wish to enable ONLY the host(s)  
specified, disable all access paths (DISABLE_ACCESS=ALL), then  
again enable the ones specified
```

3. If you do not recall a target host connection name, use the following CLI command:

```
SHOW CONNECTION
```

You will see a display similar to that in Example Display 9.

Example Display 9

```
BuildngBTop> show connection
```

Connection Name	Operating system	Controller	Port	Address	Status	Unit Offset
BUILDNGAA	PPRC_TARGET HOST_ID=5000-1FE1-0000-01F0	THIS	2	offline	0	ADAPTER_ID=5000-1FE1-0000-01F4
BUILDNGAB	PPRC_TARGET HOST_ID=5000-1FE1-0000-01F0	OTHER	2	offline	0	ADAPTER_ID=5000-1FE1-0000-01F2
BUILDNGAC	PPRC_INITIATOR HOST_ID=5000-1FE1-0000-01F0	THIS	2	220413 OL this	0	ADAPTER_ID=5000-1FE1-0000-01F4
BUILDNGAD	PPRC_INITIATOR HOST_ID=5000-1FE1-0000-01F0	OTHER	2	250413 OL other	0	ADAPTER_ID=5000-1FE1-0000-01F2

```

HOSTA1           WINNT           THIS           1           260013    OL this       0
                   HOST_ID=1000-0000-C920-A7B9    ADAPTER_ID=1000-0000-C920-A7B9

HOSTA2           WINNT           OTHER          1           200013    OL other      0
                   HOST_ID=1000-0000-C921-3F4E    ADAPTER_ID=1000-0000-C921-3F4E

HOSTB1           WINNT           THIS           1           220013    OL this       0
                   HOST_ID=1000-0000-C921-3E98    ADAPTER_ID=1000-0000-C921-3E98

HOSTB2           WINNT           OTHER          1           250013    OL other      0
                   HOST_ID=1000-0000-C921-3EFC    ADAPTER_ID=1000-0000-C921-3EFC
    
```

- ④ 4. After you have given the target site hosts access, perform the following CLI command to verify the access:

```
SHOW UnitName
```

You will see a display similar to that in Example Display 10.

Example Display 10

```

BuildngBTop> show d1
LUN                                     Uses                                     Used by
-----
D1                                     DISK10000                               BUILDNGB\RCS1
LUN ID:          6000-1FE1-0000-4250-0009-9411-5654-003E
NOIDENTIFIER
Switches:
  RUN              NOWRITE_PROTECT          READ_CACHE
  READAHEAD_CACHE  WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD,  HOSTB1,  HOSTB2
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = THIS_CONTROLLER
Size:          17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
    
```

- ④ 5. Verify that the target hosts can connect to the LUNs with this command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 11.

Example Display 11

```

BuildngBTop> show units full
LUN                               Uses                               Used by
-----
D1                                  DISK10000                          BUILDNGB\RCS1
LUN ID:        6000-1FE1-0000-4250-0009-9411-5654-003E
NOIDENTIFIER
Switches:
  RUN                               NOWRITE_PROTECT                      READ_CACHE
  READAHEAD_CACHE                   WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD,      HOSTB1,      HOSTB2
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = THIS_CONTROLLER
Size:          17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )

D2                                  DISK20000                          BUILDNGA\RCS2
LUN ID:        6000-1FE1-0000-4250-0009-9411-5654-003F
NOIDENTIFIER
Switches:
  RUN                               NOWRITE_PROTECT                      READ_CACHE
  READAHEAD_CACHE                   WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD,      HOSTB1,      HOSTB2
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = OTHER_CONTROLLER
  Target NORMAL
Size:          17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )

```

In the Access field of the display, all units that are used by remote copy sets will show that the target host connections are enabled. The display should also show the initiator controller connections.

6. Allow hosts to recognize new units. Follow the steps listed below for each operating system in your heterogeneous configuration:

- a. **Compaq OpenVMS:** If the target site hosts are shut down, boot them now. Booting the hosts enables OpenVMS to recognize the drives.

If the target site hosts are not shut down, use the following command from a privileged account to enable OpenVMS to recognize the drives:

```
MCR SYSMAN IO AUTOCONFIGURE/LOG
```

- b. **Compaq Tru64 UNIX:** If the target site hosts are shut down, boot them now. Booting the hosts enables Tru64 UNIX to recognize the drives.

If the target site hosts are not shut down, use the following command to recognize the drives:

```
hwmgr - scan scsi
```

This might take a while for large configurations. If this is the case, scan only those SCSI buses that have new units added. Scan only one bus at a time. Use the following command:

```
hwmgr -scan scsi -bus x
```

where *x* is the SCSI bus number.

c. **HP-UX:**

- 1) If the target site hosts are shut down, boot them now. Booting the hosts enables HP-UX to recognize the drives.

If the target site hosts are not shut down, use the following command to enable HP-UX to recognize the drives and verify that they are present. This command will display only the previously configured failed-over LUNs:

```
ioscan -fnCdisk
```

- 2) Continue with the following commands to access file systems on new failed-over LUNs. If you have no new failed-over LUNs, skip these substeps and go directly to the next step to mount the LUNs:

- a. `/opt/CPQswsp/spmgr display -u`

- b. `/opt/CPQswsp/spmgr add WWN`

Repeat this command for each un-attached WWN that was displayed.

- c. `ioscan -fnCdisk`

If the device special files were not displayed, run `insf -e`, then run `ioscan -fnCdisk` again.

- d. `vgimport VolumeGroupName DeviceSpecialFile`

Repeat this command for each new failed-over LUN.

- 3) Use the following command to mount the LUNs:

```
mount -a
```

NOTE: *VolumeGroupName* is the name of the volume group you originally created at the initiator site. The *DeviceSpecialFiles* are from the `ioscan` in the form of `/dev/dsk/c_t_d_`.

For consistency, configure the same *DeviceSpecialFiles* with the same volume groups, logical volumes, and file systems for the failed-over LUNs at the target site with the same LUNs at the initiator site.

- d. **IBM AIX:** If the target site hosts are shut down, boot them now. Booting the hosts enables IBM AIX to recognize the drives.

If the target site hosts are not shut down, use the following commands to enable AIX to recognize the drives and verify that they are present:

```
cfgmgr -v  
lsdev -Cc disk
```

Use the following commands to access file systems on the failed-over LUNs:

```
importvg -y volumeGroupName hdiskx  
mount all
```

NOTE: *volumeGroupName* is the name of the volume group you originally created at the initiator site, and *x* is the number of the hdisk assigned to the failed-over LUN. If the *-y volumeGroupName* parameter is omitted, AIX will create a default volume group name for you, for example, *vg00*.

- e. **Microsoft Windows NT-X86:** Reboot the hosts at the target site and log in using an account that has administrative privileges. You should be able to see all of the units by choosing **My Computer**.
- f. **Microsoft Windows 2000:**
- 1) If you *have not* changed the UNIT_OFFSET of any host connections since the hosts have been booted, you do not need to reboot the initiator site hosts.
 - a) On each host, log in using an account that has administrative privileges.
 - b) Open **Computer Management** and click **Disk Management**.
 - c) After **Disk Management** has initialized, go to the **Action** menu and click **Rescan Disks**. All of the failed over units should appear in the right-hand pane. If Secure Path is not installed correctly, you will see each unit twice.
 - 2) If you *have* changed the UNIT_OFFSET of any host connections, you must reboot that host. After the server has rebooted, log in using an account that has administrative privileges. You will see all of the units in **Computer Management > Disk Management**. If Secure Path is not installed correctly, you will see each drive twice.
- g. **Novell NetWare:** If the target site hosts are shut down, boot them now. If you are using traditional NetWare volumes, booting the hosts allows Novell NetWare to recognize the drives and automatically mount the volumes. If you

are using NSS logical volumes, booting the hosts will recognize the NSS pools and activate them. However, you must manually mount each individual NSS volume by typing `MOUNT VolumeName` at the NetWare console.

If the target site hosts are already up and running, or if they do not recognize the drives, issue the following command from the console before mounting the volumes:

```
SCAN FOR NEW DEVICES
```

Alternatively, you can use the `NWCONFIG` utility to issue this same command.

Next, mount the volumes with these commands:

```
MOUNT ALL (for traditional NetWare volumes)
```

```
MOUNT VolumeName (for NSS logical volumes).
```

- h. **SUN Solaris:** Reboot the hosts using the command `reboot -- -r` at the target site and log in using an account that has administrative privileges. You should be able to see all of the units by using the `format` command.

If Secure Path was not configured for these units, you will not see the drives. You will need to edit the WWLIDs in the file `/kernel/drv/ldLite.conf`. To find the new WWLIDs of the units, use the `SHOW Unitname` command on the controller. You may also need to adjust the files `/kernel/drv/mda.conf` and `/kernel/drv/sd.conf` to accommodate the extras LUNs. When you have edited `ldLite.conf`, `mda.conf`, and `sd.conf`, reboot the host using the `reboot -- -r` command. You should now be able to see the drives using the `format` command. Refer to the *Compaq SANworks Secure Path for Sun Solaris Installation and Reference Guide* for additional assistance.

This completes the Role Reversal Failover. The next section describes the Role Reversal Failback from a Role Reversal Failover.

Role Reversal Failback

The Role Reversal Failback is used in conjunction with the Role Reversal Failover Procedure. The Role Reversal Failback consists of the following procedures:

- Target Site Failback Procedure
- Initiator Site Cleanup Procedure

Target Site Failback Procedure

- ① 1. Shut down the target site hosts (this is not necessary for Compaq OpenVMS, Compaq Tru64 UNIX, HP-UX, IBM AIX, Sun Solaris, and Novell Netware operating systems).

IMPORTANT: If hosts are not shut down, you must remove host access on all LUNs used with remote copy sets.
- ② 2. Disable host access to the target units for all remote copy sets with the following CLI command:


```
SET UnitName DISABLE = TargetHostConnectionNamex,  
TargetHostConnectionNamey
```

Example: set d1 disable = hostb1,hostb2

Repeat this step for all units.
- ③ 3. You may now boot hosts for non-remote copy set units.
- ④ 4. Turn off write history logging, if enabled, with the following CLI command:


```
SET AssociationSetName NOLOG_UNIT
```

Example: set as_d1 nolog_unit

Repeat this procedure for each association set.
- ⑤ 5. Delete association sets with the following CLI command:


```
DELETE AssociationSetName
```

Example: delete as_d1

Repeat this procedure for each association set.
- ⑥ 6. Move control of the remote copy sets to the original initiator with the following CLI command:


```
SET RemoteCopySetName INITIATOR = InitiatorRemoteCopyName\UnitName
```

Example: set rcs1 initiator = buildnga\d1

NOTE: If after issuing this command for one of the remote copy sets, you get the error message: Error: Rem Cp Set specified is currently in a transient state, wait a few seconds and try again. The command will eventually succeed.

- 7. Verify original initiator control with the following CLI command:

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to that in Example Display 13.

Example Display 12

```
BuildngBTop> show remote_copy_sets full
No REMOTE_COPY_SETS
```

Repeat this step for all remote copy sets.

- 8. If maximum cached transfer size was changed for the target units as part of the failover procedure, set it back to 128 with the following CLI command:

```
SET UnitName MAXIMUM_CACHED_TRANSFER_SIZE = 128
```

Example: set d1 maximum_cached_transfer_size = 128

- 9. Verify the change with the following CLI command:

```
SHOW UnitName
```

You will see a display similar to that in Example Display 13.

Example Display 13

```
BuildngBTop> show d1
LUN                               Uses                               Used by
-----
D1                                  DISK10000                          BUILDNGA\RCS1
LUN ID:                            6000-1FE1-0000-4250-0009-9411-5654-003E
NOIDENTIFIER
Switches:
  RUN                                NOWRITE_PROTECT                      READ_CACHE
  READAHEAD_CACHE                    WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 128
  MAX_WRITE_CACHED_TRANSFER_SIZE = 128
Access:
  BUILDNGAA, BUILDNGAB, BUILDNGAC, BUILDNGAD
State:
  ONLINE to the other controller
  PREFERRED_PATH = THIS_CONTROLLER
  Target NORMAL
Size:                                17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
```

NOTE: This command sets both the read and write maximum cached transfer size.

Repeat this procedure for each unit.

- ⑩ 10. Continue with the Role Reversal Failback procedure at the initiator site with Initiator Site Cleanup Procedure.

Initiator Site Cleanup Procedure

- ▶ 1. If you wish, you can enhance host I/O performance by resetting the maximum cached transfer size to the original value used on the initiator. Use this command:

```
SET UnitName MAXIMUM_CACHED_TRANSFER_SIZE = InitiatorValue
```

```
Example: set d1 maximum_cached_transfer_size = 32
```

- ▶ 2. Verify the change of maximum cached transfer size to the original value by issuing the following CLI command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 14.

Example Display 14

```
BuildngATop> show units full
-----
```

LUN	Uses	Used by
D1	DISK10000	BUILDNGA\RCS1
LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0134 NOIDENTIFIER Switches: RUN NOWRITE_PROTECT READ_CACHE READAHEAD_CACHE WRITEBACK_CACHE MAX_READ_CACHED_TRANSFER_SIZE = 32 MAX_WRITE_CACHED_TRANSFER_SIZE = 32 Access: BUILDNGBA, BUILDNGBB, BUILDNGBC, BUILDNGBD State: ONLINE to the other controller PREFERRED_PATH = THIS_CONTROLLER Size: 17769177 blocks Geometry (C/H/S): (5258 / 20 / 169)		
D2	DISK20000	BUILDNGA\RCS2
LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0135 NOIDENTIFIER Switches: RUN NOWRITE_PROTECT READ_CACHE READAHEAD_CACHE WRITEBACK_CACHE MAX_READ_CACHED_TRANSFER_SIZE = 32 MAX_WRITE_CACHED_TRANSFER_SIZE = 32 Access: BUILDNGBA, BUILDNGBB, BUILDNGBC, BUILDNGBD State: ONLINE to the other controller PREFERRED_PATH = OTHER_CONTROLLER Size: 17769177 blocks Geometry (C/H/S): (5258 / 20 / 169)		
D10	MIR_DLOG	
LUN ID: 6000-1FE1-0000-01F0-0009-8490-6303-0181		

```

NOIDENTIFIER
Switches:
  RUN                      NOWRITE_PROTECT          READ_CACHE
  READAHEAD_CACHE         NOWRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 32
  MAX_WRITE_CACHED_TRANSFER_SIZE = 32
Access:
  None
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = THIS_CONTROLLER
Size:          17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
    
```

- ▶ 3. Create association sets and then add the log unit, if desired. For information on how to create association sets, with or without write history logging, see Appendix C.

IMPORTANT: If you will be using scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention (remote copy sets, stripesets, mirrorsets, RAIDsets, association sets, and connections)—use underscores instead. Dashes are not allowed by the Perl scripting language.

- ▶ 4. When you have created the association set, verify the creation with the following CLI command:

```
SHOW ASSOCIATION_SETS FULL
```

You will see a display similar to that in Example Display 15.

Example Display 15

```

BuildngATop> show association full
Name          Association          Uses          Used by
-----
AS_D1         association          RCS1
Switches:
  NOFAIL_ALL
  NOORDER_ALL
  LOG_UNIT = D10 (No data logged)
    
```

- ▶ 5. Enable access to the initiator site host by using the following CLI command:

```
SET UnitName ENABLE = InitiatorHostConnectionNamex,
InitiatorHostConnectionNamey
```

Example: set d1 enable = hosta1,hosta2

- ▶ 6. Allow hosts to recognize new units. Follow the steps listed below for each operating system in your heterogeneous configuration:
 - a. **Compaq OpenVMS:** If the initiator site hosts are shut down, boot them now. Booting the hosts enables OpenVMS to recognize the drives.

If the initiator site hosts are not shut down, use the following command from a privileged account to enable OpenVMS to recognize the drives:

```
MCR SYSMAN IO AUTOCONFIGURE/LOG
```

- b. **Compaq Tru64 UNIX:** If the initiator site hosts are shut down, boot them now. Booting the hosts enables Tru64 UNIX to recognize the drives.

If the initiator site hosts are not shut down, use the following command to recognize the drives:

```
hwmgr - scan scsi
```

This might take a while for large configurations. If this is the case, scan only those SCSI buses that have new units added. Scan only one bus at a time. Use the following command:

```
hwmgr -scan scsi -bus x
```

where x is the SCSI bus number.

- c. **HP-UX:** If the initiator site hosts are shut down, boot them now. Booting the hosts enables HP-UX to recognize the drives.

If the initiator site hosts are not shut down, use the following commands to recognize the drives and mount the file systems:

```
ioscan -fnCdisk
```

```
mount -a
```

- d. **IBM AIX:** If the initiator site hosts are shut down, boot them now. Booting the hosts enables IBM AIX to recognize the drives.

If the initiator site hosts are not shut down, use the following commands to recognize the drives and mount the file systems:

```
cfgmgr -v
```

```
mount all
```

- e. **Microsoft Windows NT-X86:** Reboot the hosts at the initiator site and log in using an account that has administrative privileges. You should be able to see all of the units by choosing **My Computer**.

- f. **Microsoft Windows 2000:**

- 1) If you *have not* changed the UNIT_OFFSET of any host connections since the hosts have been booted, you do not need to reboot the initiator site hosts.

- a) On each host, log in using an account that has administrative privileges.

- b) Open **Computer Management** and click **Disk Management**.
 - c) After **Disk Management** has initialized, go to the **Action** menu and click **Rescan Disks**. All of the failed over units should appear in the right-hand pane. If Secure Path is not installed correctly, you will see each unit twice.
- 2) If you *have* changed the UNIT_OFFSET of any host connections, you must reboot that host. After the server has rebooted, log in using an account that has administrative privileges. You will see all of the units in **Computer Management > Disk Management**. If Secure Path is not installed correctly, you will see each drive twice.
- g. **Novell NetWare:** If the initiator site hosts are shut down, boot them now. Booting the hosts allows Novell NetWare to recognize the drives.

If the initiator site hosts are already up and running, or if they do not recognize the drives, issue the following command from the console before mounting the volumes:

```
SCAN FOR NEW DEVICES
```

Alternatively, you can use the `NWCONFIG` utility to issue this same command.

- h. **SUN Solaris:** Reboot the hosts using the command `reboot -- -r` at the initiator site and log in using an account that has administrative privileges. You should be able to see all of the units by using the `format` command.

If Secure Path was not configured for these units, you will not see the drives. You will need to edit the WWLIDs in the file `/kernel/drv/ldLite.conf`. To find the new WWLIDs of the units, use the `SHOW Unitname` command on the controller. You may also need to adjust the files `/kernel/drv/mda.conf` and `/kernel/drv/sd.conf` to accommodate the extras LUNs. When you have edited `ldLite.conf`, `mda.conf`, and `sd.conf`, reboot the host using the `reboot -- -r` command. You should now be able to see the drives using the `format` command. Refer to the *Compaq SANworks Secure Path for Sun Solaris Installation and Reference Guide* for additional assistance.

This completes the Role Reversal Failback Procedure.

Disaster Recovery After Role Reversal Procedure

This chapter contains these procedures to follow when you are performing the role reversal procedure in Chapter 10 and the access to the target site has been lost. The following steps will tell you how to failback to the controller at the initiator, and, when access to the target has been regained, how to re-create the remote copy sets so that data is copied from the initiator to the target site.

- “Role Reversal Unplanned Failback” on page 11–2
 - “Initiator Site Preparation Procedure” on page 11–2
 - “Target Site Cleanup Procedure” on page 11–6
 - “Initiator Site Cleanup Procedure” on page 11–6

NOTE: In this chapter, *initiator* site procedure steps are identified by an arrow symbol ► in the margin. *Target* site procedure steps are identified by a target symbol ☉ in the margin.

NOTE: Some example displays illustrate confirmation messages with the event log symbol (%EVL) and an instance code. Compare the instance code in the example with the instance code you receive. If the numbers are the same, you have performed the previous command correctly and have achieved the desired results. Note that you will be able to see these screens only if you are working from the controller to which the LUNs are online. Refer to the Troubleshooting chapter for more information on instance codes and their meanings.

Example displays may also contain bold text to identify information that is the most pertinent in the example. In many cases, items shown in bold text will help you verify the results of a previous command.

Role Reversal Unplanned Failback

The Role Reversal Unplanned Failback is used as an alternative to the Role Reversal Failback in Chapter 10.

Initiator Site Preparation Procedure

- ▶ 1. Before performing the failback procedure, locate your record of `SHOW` command output that details the current initiator configuration.

Verify that your target controller configuration is the same as your initiator controller configuration. Compare the status of the controllers, association sets, remote copy sets, units, and connections. Appendix A contains the full procedure.

- ▶ 2. Disconnect remote controller access with the following CLI commands:

```
SET THIS_CONTROLLER PORT_2_TOPOLOGY = OFFLINE
SET OTHER_CONTROLLER PORT_2_TOPOLOGY = OFFLINE
```

- ▶ 3. Verify remote controller disconnection with the following CLI commands:

```
SHOW THIS_CONTROLLER
SHOW OTHER_CONTROLLER
```

You will see a display similar to that in Example Display 1.

Example Display 1

```
BuildngATop> show this_controller
Controller:
  HSG80 ZG84906303 Software V86-1P, Hardware E03
  NODE_ID = 5000-1FE1-0000-01F0
  ALLOCATION_CLASS = 0
  SCSI_VERSION = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG84906237
  In dual-redundant configuration
  Device Port SCSI address 7
  Time: 10-MAY-2001 17:55:29
  Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-01F3
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address = 220213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-01F4
  PORT_2_TOPOLOGY = OFFLINE (offline)
  REMOTE_COPY = BUILDNGA
.
.
.
```

```

BuildngBTop> show other_controller
Controller:
  HSG80 ZG94319198 Software V86-1P, Hardware E10
  NODE_ID           = 5000-1FE1-0000-4250
  ALLOCATION_CLASS   = 0
  SCSI_VERSION      = SCSI-3
  Configured for MULTIBUS_FAILOVER with ZG94115654
  In dual-redundant configuration
  Device Port SCSI address 6
  Time: 10-MAY-2001 16:43:12
  Command Console LUN is lun 0 (NOIDENTIFIER)
Host PORT_1:
  Reported PORT_ID = 5000-1FE1-0000-4251
  PORT_1_TOPOLOGY = FABRIC (fabric up)
  Address          = 200213
Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0000-4252
  PORT_2_TOPOLOGY = OFFLINE (offline)
  REMOTE_COPY     = BUILDNGB
.
.
.

```

- ▶ 4. Delete the remote copy sets with the following CLI command:

```
DELETE RemoteCopySetName
```

Example: delete rcs1

Repeat this step for all units.

- ▶ 5. Enable access from the initiator host to the storage units with the following CLI command:

```
SET UnitName ENABLE = InitiatorHostConnectionNamex,
InitiatorHostConnectionNamey
```

Example: set d1 enable = hosta1,hosta2

Repeat this step for all units.

- ▶ 6. Allow hosts to recognize new units. Follow the steps listed below for each operating system in your heterogeneous configuration:

- a. **Compaq OpenVMS:** If the initiator site hosts are shut down, boot them now. Booting the hosts enables OpenVMS to recognize the drives.

If the initiator site hosts are not shut down, use the following command from a privileged account to enable OpenVMS to recognize the drives:

```
MCR SYSMAN IO AUTOCONFIGURE/LOG
```

- b. **Compaq Tru64 UNIX:** If the initiator site hosts are shut down, boot them now. Booting the hosts enables Tru64 UNIX to recognize the drives.

If the initiator site hosts are not shut down, use the following command to recognize the drives:

```
hwmgr - scan scsi
```

This might take a while for large configurations. If this is the case, scan only those SCSI buses that have new units added. Scan only one bus at a time. Use the following command:

```
hwmgr -scan scsi -bus x
```

where x is the SCSI bus number.

- c. **HP-UX:** If the initiator site hosts are shut down, boot them now. Booting the hosts enables HP-UX to recognize the drives.

If the initiator site hosts are not shut down, use the following commands to recognize the drives and mount the file systems:

```
ioscan -fnCdisk
```

```
mount -a
```

- d. **IBM AIX:** If the initiator site hosts are shut down, boot them now. Booting the hosts enables IBM AIX to recognize the drives.

If the initiator site hosts are not shut down, use the following commands to recognize the drives and mount the file systems:

```
cfgmgr -v
```

```
mount all
```

- e. **Microsoft Windows NT-X86:** Reboot the hosts at the initiator site and log in using an account that has administrative privileges. You should be able to see all of the units by choosing **My Computer**.

- f. **Microsoft Windows 2000:**

- 1) If you *have not* changed the UNIT_OFFSET of any host connections since the hosts have been booted, you do not need to reboot the initiator site hosts.

- a) On each host, log in using an account that has administrative privileges.

- b) Open **Computer Management** and click **Disk Management**.

- c) After **Disk Management** has initialized, go to the **Action** menu and click **Rescan Disks**. All of the failed over units should appear in the right-hand pane. If Secure Path is not installed correctly, you will see each unit twice.

2) If you *have* changed the UNIT_OFFSET of any host connections, you must reboot that host. After the server has rebooted, log in using an account that has administrative privileges. You will see all of the units in **Computer Management > Disk Management**. If Secure Path is not installed correctly, you will see each drive twice.

- g. **Novell NetWare:** If the initiator site hosts are shut down, boot them now. Booting the hosts allows Novell NetWare to recognize the drives.

If the initiator site hosts are already up and running, or if they do not recognize the drives, issue the following command from the console before mounting the volumes:

```
SCAN FOR NEW DEVICES
```

Alternatively, you can use the `NWCONFIG` utility to issue this same command.

- h. **SUN Solaris:** Reboot the hosts using the command `reboot -- -r` at the initiator site and log in using an account that has administrative privileges. You should be able to see all of the units by using the `format` command.

If Secure Path was not configured for these units, you will not see the drives. You will need to edit the WWLIDs in the file `/kernel/drv/ldLite.conf`. To find the new WWLIDs of the units, use the `SHOW Unitname` command on the controller. You may also need to adjust the files `/kernel/drv/mda.conf` and `/kernel/drv/sd.conf` to accommodate the extras LUNs. When you have edited `ldLite.conf`, `mda.conf`, and `sd.conf`, reboot the host using the `reboot -- -r` command. You should now be able to see the drives using the `format` command. Refer to the *Compaq SANworks Secure Path for Sun Solaris Installation and Reference Guide* for additional assistance.

- ▶ 7. If desired, you may now begin I/O operations at the initiator site.
- ▶ 8. When you have repaired the target site and it is operational, proceed to the Target Site Cleanup Procedure.

Target Site Cleanup Procedure

- ① 1. Shut down the target site hosts (this is not necessary for Compaq OpenVMS, Compaq Tru64 UNIX, HP-UX, IBM AIX, Novell Netware, and Sun Solaris operating systems).
IMPORTANT: If hosts are not shut down, you must stop I/O and unmount the volumes from the hosts.
- ② 2. Disconnect remote controller access with the following CLI commands:

```
SET THIS_CONTROLLER PORT_2_TOPOLOGY = OFFLINE  
SET OTHER_CONTROLLER PORT_2_TOPOLOGY = OFFLINE
```
- ③ 3. Disable host access to the target remote copy set units with the following CLI command.

```
SET UnitName DISABLE = TargetHostConnectionNamex,  
TargetHostConnectionNamey
```

Example: set d1 disable = hostb1,hostb2

Repeat this step for all remote copy set units.
- ④ 4. You may now boot all hosts.
- ⑤ 5. Delete the remote copy sets with this CLI command:

```
DELETE RemoteCopySetName
```

Example: delete rcs1

Repeat this step for all units.
- ⑥ 6. Reconnect remote controller access with the following CLI commands:

```
SET THIS_CONTROLLER PORT_2_TOPOLOGY = FABRIC  
SET OTHER_CONTROLLER PORT_2_TOPOLOGY = FABRIC
```
- ⑦ 7. When the target site has been cleaned up, proceed to the Initiator Site Cleanup Procedure.

Initiator Site Cleanup Procedure

- ▶ 1. To restore the connection to the fabric, issue the following CLI commands:

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


- ▶ 2. Verify remote controller access with the following CLI command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 2.

Example Display 2

```
BuildngATop> show units full
LUN                               Uses                               Used by
-----
D1                                DISK10000                          INT\RCS1
LUN ID:        6000-1FE1-0001-3B10-0009-9341-3895-0060
NOIDENTIFIER
Switches:
  RUN                               NOWRITE_PROTECT                      READ_CACHE
  READAHEAD_CACHE                   WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 128
  MAX_WRITE_CACHED_TRANSFER_SIZE = 128
Access:
  HOST1A,  HOST1B,  BUILDINGBA,  BUILDINGBB,
  BUILDINGBC,  BUILDINGBD
State:
  ONLINE to the other controller
  PREFERRED_PATH = OTHER_CONTROLLER
Size:        17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
```

- ▶ 3. Check all units for lost data with the following CLI command:

```
SHOW UNITS FULL
```

If there are units with lost data, you will see a display similar to that in Example Display 3.

Example Display 3

```
BuildngATop> show units full
LUN                               Uses                               Used by
-----
D1                                DISK10000                          Buildnga\RCS1
LUN ID:        6000-1FE1-0007-9DD0-0009-0510-3907-000C
NOIDENTIFIER
Switches:
  RUN                               NOWRITE_PROTECT                      READ_CACHE
  READAHEAD_CACHE                   WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 128
  MAX_WRITE_CACHED_TRANSFER_SIZE = 128
Access:
  HOST1A,  HOST1B,  BUILDINGBA,  BUILDINGBB,
  BUILDINGBC,  BUILDINGBD
State:
INOPERATIVE
Unit has lost data
UNKNOWN - Unit is no longer an initiator
PREFERRED_PATH = THIS_CONTROLLER
WRITE_PROTECT - DATA SAFETY
```

Size: NOT YET KNOWN
 Geometry (C/H/S): NOT YET KNOWN

- a. If there are units with lost data, clear the data for each applicable unit, with the following CLI command:

```
CLEAR_ERRORS UnitName LOST_DATA
```

Example: `clear_errors d1 lost_data`

- b. Verify that all the lost data has been cleared with the following CLI command:

```
SHOW UNITS FULL
```

You will see a display similar to that in Example Display 4. When the lost data has been cleared, the display will indicate that the unit is ONLINE.

Example Display 4

```
BuildngATop> show units full
LUN                               Uses                               Used by
-----
D1                                  DISK10000                          BUILDNGA\RCS1
LUN ID:        6000-1FE1-0000-01F0-0009-8490-6303-0134
NOIDENTIFIER
Switches:
  RUN                NOWRITE_PROTECT                READ_CACHE
  READAHEAD_CACHE   WRITEBACK_CACHE
  MAX_READ_CACHED_TRANSFER_SIZE = 128
  MAX_WRITE_CACHED_TRANSFER_SIZE = 128
Access:
  HOST1A,  HOST1B,  BUILDINGBA,  BUILDINGBB,
  BUILDINGBC,  BUILDINGBD
State:
ONLINE to the other controller
UNKNOWN - Unit is no longer an initiator
PREFERRED_PATH = THIS_CONTROLLER
Size:        17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )
```

4. Recreate your remote copy sets with the following CLI command:

```
ADD REMOTE_COPY_SETS RemoteCopySetName UnitName
TargetRemoteCopyName\UnitName
```

Example: `add remote_copy_sets rcs1 d1 buildingb\d1`

Repeat this step for all remote copy sets.

5. Verify that you have created all of your remote copy sets correctly with the following CLI command:

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to Example Display 5.

Example Display 5

```
BuildngATop> show remote_copy_sets full
      LUN                               Uses                               Used by
-----
RCS1      remote copy                    D1                               AS1
Reported LUN ID: 6000-1FE1-0001-3B10-0009-9341-3895-0060
Switches:
  OPERATION_MODE = SYNCHRONOUS
  ERROR_MODE     = NORMAL
  FAILOVER_MODE  = MANUAL
  OUTSTANDING_IOS = 200
Initiator (BUILDNGA\D1) state:
  ONLINE to this controller
  Not reserved
Target state:
  BUILDNGE\D1      is NORMAL
```

- ▶ 6. If desired, set the remote copy set into asynchronous mode by issuing the following CLI command:

```
SET RemoteCopySetName OPERATION_MODE = ASYNCHRONOUS
```

Example: `set rcs1 operation_mode = asynchronous`

Repeat this step for all applicable remote copy sets.

- ▶ 7. Obtain your record of SHOW command output that details the original initiator configuration. Using the output as a reference, create association sets and set up write history logging to duplicate those that were on the initiator. For information on how to create association sets, see Appendix C.

Repeat this step for each applicable association set.

IMPORTANT: If you will be using scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention (remote copy sets, stripesets, mirrorsets, RAIDsets, association sets, and connections)—use underscores instead. Dashes are not allowed by the Perl scripting language.

When you have created the association sets, verify their creation with the following CLI command:

```
SHOW ASSOCIATIONS FULL
```

You will see a display similar to Example Display 6.

Example Display 6

```
BuildngATop> show associations full
Name Association Uses Used by
-----
AS_D1 association RCS1
Switches:
NOFAIL_ALL
NOORDER_ALL
LOG_UNIT = D10 (no data logged)
```

- ▶ 8. Re-enable failsafe mode, if desired. To set failsafe mode, enter the following CLI command:

```
SET RemoteCopySetName ERROR_MODE = FAILSAFE
```

Example: `set rcs1 error_mode = failsafe`

Repeat this step for all applicable remote copy sets.

NOTE: Failsafe cannot be set if the remote copy set is in an association set that will be used for write history logging.

This completes the Role Reversal Unplanned Failback.

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 a Data Replication Manager 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 during failover and failback are discussed.

Troubleshooting information on the HSG80 controller can be found in the *Compaq StorageWorks HSG80 Array Controller Version 8.6 Troubleshooting Reference Guide*. Troubleshooting information specific to the DRM configuration process can be found in the *SANworks Data Replication Manager by Compaq HSG80 ACS Version 8.6-4P Configuration User Guide*. Troubleshooting information on specific Data Replication Manager components can also be found in their respective user manuals.

This chapter contains the following topics:

- “HSG80 Array Controller Operating Characteristics” on page 12–2
 - “Forced Errors Detected During Copy” on page 12–2
 - “Read Errors Detected During Full Copy” on page 12–2
 - “Dual Redundancy During Failback” on page 12–2
 - “Failsafe Lock Management” on page 12–3
 - “Link Failure Management” on page 12–3
 - “Remote Copy Set Member Failures” on page 12–3
 - “Remote Copy Set World Wide LUN ID” on page 12–4
 - “Write History Logging” on page 12–4
 - “Component Failures” on page 12–4
- “Failure Modes of a DT System in Normal Operation” on page 12–6
 - “Failure at Target Site After Failover” on page 12–7
- “Confirmation Message Instance Codes” on page 12–8

HSG80 Array Controller Operating Characteristics

The HSG80 array 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 should be restored from a known good backup.

Refer to the *Compaq StorageWorks HSG80 Array Controller ACS V8.6 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, when a read error is detected an unrecoverable error is reported to the host, the offending block is re-vectored, 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 *SANworks Data Replication Manager by Compaq HSG80 ACS Version 8.6-4P Configuration User Guide* and to the *Compaq StorageWorks HSG80 Array Controller ACS V8.6 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 for a remote copy set, that set can become failsafe locked if a unit fails or the target becomes inaccessible.

If a unit fails at the target site, then the target is removed from the remote copy set, and the remote copy set is placed in a failsafe lock condition. Once the unit failure has been eliminated, you can re-add the target to the remote copy set that initiates a full copy.

If a dual-link failure occurs, the remote copy set is placed in a failsafe locked condition. The target remains a member of the remote copy set but is marked invalid. Once the link has been restored to the target, a full copy is initiated. Once completed, the failsafe locked condition is cleared.

If the initiator unit fails, the remote copy set goes into failsafe locked condition.

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 is removed, and, if the remote copy set was in failsafe error mode, then 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/write accessible through the initiator controller. Recovery from this condition requires a failover to the target site.

Remote Copy Set World Wide LUN ID

Remote copy sets are assigned a unique world wide 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 have had a failover to the target site.

Write History Logging

Once write history logging commences to a log unit, care must be taken when choosing to disable logging. Issuing the `SET AssociationSetName NOLOG_UNIT` command may incur a full copy operation on the remote copy set. For example, this may happen if the controller is logging updates for a remote copy set because the links to the target are down. If the log unit is disabled during this time, the controller cannot use the write history log to update the target when the links are restored, as some operations were not written to the log. Therefore, a full copy is initiated. Also, the log disk is no longer known to the controller.

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 disaster-tolerant (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 to 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 (Data Replication Manager Services Event Sense Data Response). Refer to the *Compaq StorageWorks HSG80 Array Controller ACS V8.6 Maintenance and Service Guide* for more information.

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 can manipulate controllers and storage through the GUI and can intervene in the DT process when there is a problem.

Refer to the *Compaq StorageWorks Command Console User Guide* and the on-line user help for more information.

Failure of One Member in a Dual Redundant Controller Pair

In a dual redundant setup, 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 Modes of a DT System in Normal Operation

Table 12–1 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 12–1: Failure Modes of a DT System with Normal Operation

Initiator Host	Target Host	Initiator Switch A	Initiator Switch B	Target Switch A	Target Switch B	Initiator Controller A	Initiator Controller B	Target Controller A	Target Controller B	Failure Mode	Action
Loss of:											
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 mini-merge or full copy
		X		X						Data path	Repair switches
						X				Data path	Repair controller
							X			Data path	Repair controller

Table 12–1: Failure Modes of a DT System with Normal Operation (Continued)

Initiator Host	Target Host	Initiator Switch A	Initiator 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	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 in the same way as in a non-disaster tolerant state. Table 12–2 shows the possible failure modes at the target site, assuming that the initiator site is not available to failback to.

Table 12–2: Target Site DT Failure Modes After Failover

Target Host	Target Top Switch	Target Bottom Switch	Target Controller A	Target Controller B	Failure Mode Loss Of	Action
X					Remote site	Repair host
	X				Data path	Repair switch

Table 12–2: Target Site DT Failure Modes After Failover (Continued)

		X			Data path	Repair switch
	X	X			Data access	Repair switches
			X		Data path	Repair controller
				X	Data path	Repair controller
			X	X	Data access	Replace controllers

Confirmation Message Instance Codes

Use this table as a guide in interpreting the instance codes in your confirmation messages. You can also find more information about these codes in the *Compaq StorageWorks HSG80 Array Controller Version 8.6 Troubleshooting Reference Guide*.

Table 12–3: Instance Code Legend

Instance Code	What It Means
02908901	The host command failed because the remote copy set went failsafe locked prior to command completion. The remote copy set is specified by the Remote Copy Name field. The Information field of the Device Sense Data contains the block number of the first block error.
07050064	Failover Control received a Last Gasp message from the other controller. The other controller is expected to restart within a given time period. If the other controller does not, the other controller will be held reset with the “Kill” line.
43010064	Host Port Protocol component has detected that the other controller has failed and that this controller has taken over the units specified in the extended sense data.
0258000A	This command was aborted prior to completion. The Information field of the Device Sense Data contains the block number of the first block in error.
0E010064	A remote copy set has been created specified by the Remote Copy Set Name field. The initiator unit of the remote copy set is specified by the initiator WWLID field.

Table 12–3: Instance Code Legend (Continued)

Instance Code	What It Means
0E020064	The remote copy set specified by the Remote Copy Set Name field has been deleted by the operator.
0E030064	The logical unit specified by the target WWLID has transitioned from the normalizing or copying state to the normal state.
0E078A01	The logical unit specified by the target WWLID has been removed from the remote copy set specified by the Remote Copy Set Name field. The target was removed by the operator.
0E088864	The remote copy set specified by the Remote Copy Set Name field has just had a membership change such that disaster tolerance failsafe error mode can now be enabled if desired.
0E098901	The remote copy set specified by the Remote Copy Set Name field has gone inoperative due to a disaster tolerance failsafe locked condition.
0E0F8B01	The copy was terminated due to a write failure on the target unit. The write failure was due to the links being down (target inaccessible). The copy will restart when at least one link is restored. The initiator unit is specified by the Initiator WWLID field.
0E110064	The logical unit specified by the target WWLID field has transitioned from the merging state to the normal state.
0E120064	The copy was terminated due to a write failure on the target unit. The write failure was due to the links being down (target inaccessible). The copy will restart when at least one link is restored. The initiator unit is specified by the Initiator WWLID field.
0E210064	The logical unit specified by the target WWLID field has transitioned from the normal state to the write history logging state due to a remote connection event (the target controllers are no longer accessible) or CLI SUSPEND command.
0E220064	The logical unit specified by the target WWLID field has transitioned from the logging state to the merging state due to a remote connection event (the target controllers are no longer accessible) or CLI RESUME command.
0E050064	The logical unit specified by the target WWLID field has been added to the remote copy set specified by the Remote Copy Set Name field. The new target member is now in the normalizing state.

Status Comparison

This appendix describes the procedure for comparing the status of:

- Controllers
- Association sets
- Remote copy sets
- Units
- Connections

Performing a status comparison consists of the following procedures:

- Target Site Terminal Emulator Session
- Issuing SHOW Commands

Compaq recommends that you update your configuration records often as changes are made to the operational versions, and that you keep a copy of the results of your status comparisons at each site for ready reference.

Target Site Terminal Emulator Session

1. Using a serial cable, connect the COM port of a laptop computer or another computer to the corresponding serial port on the HSG80 controllers.
2. Start a terminal emulator session that is capable of capturing text to a file (which will later be saved as step 6 of the Issuing SHOW Commands procedure). Use the following settings: 9600 baud, 8 bits, no parity, 1 stop bit, XON/XOFF.

Issuing SHOW Commands

1. To see the full information on this controller, issue the following CLI command:

```
SHOW THIS_CONTROLLER FULL
```

You will see a display similar to that shown in Example Display 1.

2. To see the information for all association sets known to the controller pair, issue the following CLI command:

```
SHOW ASSOCIATIONS FULL
```

You will see a display similar to that of Example Display 2 for each association set.

3. To see information for all remote copy sets known to the controller pair, issue the following CLI command:

```
SHOW REMOTE_COPY_SETS FULL
```

You will see a display similar to that in Example Display 3 for each remote copy set.

4. To see information for all units configured to the controller, issue the following CLI command:

```
SHOW UNITS FULL
```

You will see a display similar to that of Example Display 4 for each unit.

5. To see the connection name, operating system, controller, controller port, adapter ID address, online or offline status, and unit offset, issue the following CLI command:

```
SHOW CONNECTIONS
```

You will see a display similar to that of Example Display 5 for each connection.

6. Save for future reference the file started during the Terminal Emulator Session procedure. This file will contain the text captured throughout the above steps 1-5.

Example Display 1 shows a sample output from the SHOW THIS_CONTROLLER FULL command:

Example Display 1

Controller:

```
HSG80 ZG91412410 Software V85P, Hardware E05
NODE_ID           = nnnnnnnnnnn
ALLOCATION_CLASS   = 0
SCSI_VERSION      = SCSI-2
Configured for MULTIBUS_FAILOVER with ZG91416136
  In dual-redundant configuration
Device Port SCSI address 6
Time: NOT SET
Command Console LUN is lun 0 (NOIDENTIFIER)
```

Host PORT_1:

```
Reported PORT_ID = 5000-1FE1-0001-3AE1
PORT_1_TOPOLOGY = FABRIC (fabric up)
```



```

Address                = 220113

Host PORT_2:
  Reported PORT_ID = 5000-1FE1-0001-3AE2
  PORT_2_TOPOLOGY = FABRIC (fabric up)
  Address          = 220313
  REMOTE_COPY     = BuildingB

Cache:
  256 megabyte write cache, version 0012
  Cache is GOOD
  No unflushed data in cache
  CACHE_FLUSH_TIMER = DEFAULT (10 seconds)

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

Battery:
  NOUPS
  FULLY CHARGED
  Expires:

Extended information:
  Terminal speed 9600 baud, eight bit, no parity, 1 stop bit
  Operation control: 00000000 Security state code: 75184
  Configuration backup disabled
  
```

Example Display 2 shows a sample output from the SHOW ASSOCIATIONS FULL command:

Example Display 2

Name	Association	Uses	Used by
AS1	association	RC1 RC2 RC3	

Switches:
 NOFAIL_ALL
 NOORDER_ALL
 NOLOG_UNIT

Example Display 3 shows a sample output from the SHOW REMOTE_COPY_SETS FULL command:

Example Display 3

Name	Uses	Used by
RC1	D1	AS1

remote copy
 Reported LUN ID: nnnnnnnnnnnnnnnn
 Switches:
 OPERATION_MODE = SYNCHRONOUS
 ERROR_MODE = NORMAL
 FAILOVER_MODE = MANUAL

```

OUTSTANDING_IOS = 60
.
.
.

```

Example Display 4 shows a sample output from the SHOW UNITS FULL command:

Example Display 4

```

D2                                DISK10100          BuildingB\RC2
LUN ID: nnnnnnnnnnnnnnnnnnnnnnn
NOIDENTIFIER
Switches:
  RUN                               NOWRITE_PROTECT      READ_CACHE
  READAHEAD_CACHE                   WRITEBACK_CACHE
  MAXIMUM_CACHED_TRANSFER_SIZE = 1
Access:
BuildngAA, BuildngAB, BuildngAC, BuildngAD, HostCon_1, HostCon_2
State:
  ONLINE to this controller
  Not reserved
  PREFERRED_PATH = OTHER_CONTROLLER
  Target NORMAL
Size:                               17769177 blocks
Geometry (C/H/S): ( 5258 / 20 / 169 )

```

Example Display 5 shows a sample output from the SHOW CONNECTIONS command:

Example Display 5

Connection		Unit				
Name	Operating system	Controller	Port	Address	Status	Offset
!NEWCON28	WINNT	THIS	1	634000	OL this	0
		HOST_ID=1000-0000-C921-4B5B		ADAPTER_ID=1000-0000-C921-4B5B.		

DRM Power Up and Power Down

This appendix describes the procedure for powering up and powering down your DRM systems.

Power Up Data Replication Manager Systems

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



CAUTION: 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 on the Data Replication Manager systems in the sequence shown in the following procedures.

Target Site Power Up Procedure

1. Ensure that all enclosures, switches, and rack power distribution units (PDUs) have their power switches in the Off position.
2. Apply power to all PDUs.
3. Turn on the power switches for the racks from the target site.
4. Ensure that all controllers are on and functional.
5. Apply power to all Fibre Channel switches.

Initiator Site Power Up Procedure

1. Ensure that all enclosures, switches, and rack PDUs have their power switches in the Off position.
2. Apply power to all PDUs.

3. Turn on the power switches for the racks from the initiator site.
4. Ensure that all controllers are on and functional.
5. Apply power to all Fibre Channel switches.

Power Down DRM Systems

Power down the DRM systems in the sequence shown in the following procedures. If the initiator site will be powered down for a long period of time, you may need to disable cache batteries.

Initiator Site Power Down Procedure

1. Issue the following CLI commands (in this order):

```
SHUTDOWN OTHER_CONTROLLER  
SHUTDOWN THIS_CONTROLLER
```
2. Turn off the Fibre Channel switches.
3. Turn off the power to the enclosures.
4. Turn off the PDUs.

Target Site Power Down Procedure

1. Issue the following CLI commands (in this order):

```
SHUTDOWN OTHER_CONTROLLER  
SHUTDOWN THIS_CONTROLLER
```
2. Turn off the Fibre Channel switches.
3. Turn off the power to the enclosures.
4. Turn off the PDUs.

Creating a Log Unit and Association Sets

This appendix describes the procedures to:

- “Create a Log Unit” on page C–1
- “Create Association Sets and Assign a Log Unit” on page C–2

Create a Log Unit

1. Create a mirrorset for the log disk by issuing the following CLI command:

```
ADD MIRRORSETS MirrorsetName DiskName1 DiskName2
```

```
Example: add mirrorsets mir_d1log disk50100 disk60100
```

IMPORTANT: If you will be using scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention (remote copy sets, stripesets, mirrorsets, RAIDsets, association sets, and connections)—use underscores instead. Dashes are not allowed by the Perl scripting language.

NOTE: To minimize the number of devices used for logging, you can create and use one-member mirrorsets. Because the data is written to one disk, the logged data will not be protected. However, all of this data is also written to the initiator unit. In the case of a log disk failure, you would incur a full normalization, rather than a mini-merge, when access to the target is re-established.

The command to create a one-member mirrorset is the same as above, except only one disk is listed.

```
Example: add mirr mir_d1log disk50100
```

2. Initialize the mirrorset with the following CLI command:

```
INITIALIZE ContainerName
```

```
Example: initialize mir_d1log
```

3. Verify that you have created a mirrorset by issuing the following CLI command:

```
SHOW MIRRORSET
```

You will see a display similar to that in Example Display 1.

Example Display 1

Name	Storageset	Uses	Used by
MIR_D1LOG	mirrorset	DISK50100 DISK60100	

4. Present the log unit to the controller with the following CLI command:

```
ADD UNIT UnitName ContainerName
```

Example: add unit d10 mir_d1log

5. Verify that the controller recognizes the log unit by issuing the following CLI command:

```
SHOW UNITS
```

You will see a display similar to that in Example Display 2.

Example Display 2

LUN	Uses	Used by
D10	MIR_D1LOG	

Create Association Sets and Assign a Log Unit

IMPORTANT: If you will be using scripting to automate failover and failback operations, do not use dashes (hyphens) as separators in your naming convention (remote copy sets, stripesets, mirrorsets, RAIDsets, association sets, and connections)—use underscores instead. Dashes are not allowed by the Perl scripting language.

1. Create an association set with the following CLI command:

```
ADD ASSOCIATIONS AssociationSetName RemoteCopySetName
```

Example: add associations as_d1 rcs1

Repeat this step for each association set.

NOTE: You can add additional members to the association set by issuing the following CLI command:

```
Set AssociationSetName ADD = RemoteCopySetName
```

Example: set as_d1 add = rcs1

Repeat for each association set name.

2. Disable node access to the log unit with the following CLI command:

```
SET UnitNumber DISABLE_ACCESS_PATH = ALL
Example: set d10 disable_access_path = all
```

3. Disable writeback cache on log units with the following CLI command:

```
SET UnitNumber NOWRITEBACK_CACHE
Example: set d10 nowriteback_cache
```

4. Check to see that you have disabled access and writeback cache with the following command:

```
SHOW D10
```

You will see a display similar to that in Example Display 3.

Example Display 3

LUN	Uses	Used by
D10	MIR_D1LOG	
LUN ID:	6000-1FE1-0001-3B10-0009-9130-8044-0066	
IDENTIFIER =	10	
Switches:		
RUN	NOWRITE_PROTECT	READ_CACHE
READAHEAD_CACHE	NOWRITEBACK_CACHE	
MAXIMUM_CACHED_TRANSFER_SIZE =	32	
Access:		
None		
State:		
ONLINE to this controller		
Not reserved		
PREFERRED_PATH =	THIS_CONTROLLER	
Size:	35556389 blocks	
Geometry (C/H/S):	(7000 / 20 / 254)	

5. Assign the log units to the association sets with the following CLI command:

```
SET AssociationSetName LOG_UNIT = D10
Example: set as_d1 log_unit = d10
```

6. Check to see the switch status of the association set by issuing the following CLI command:

```
SHOW ASSOCIATIONS FULL
```

You will see a display similar to Example Display 4.

Example Display 4

```
BuildngBTop> show associations full
Name          Association          Uses          Used by
-----
AS_D1         association          RCS1
Switches:
  NOFAIL_ALL
  NOORDER_ALL
  LOG_UNIT = D10 (No data logged)
```

Repeat this step for each association set.

Glossary

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

ACS

An acronym for array controller software. *See* array controller software.

adapter

A hardware device that converts the protocol and hardware interface of one bus type to another without changing the function of either bus.

AL_PA

or

ALPA

An acronym for Arbitrated Loop Physical Address. A two-digit hexadecimal number that expresses a port's physical position on the loop. ALPA numbers are normally not assigned in sequence (i.e., position 1 is not ALPA 1, and so on). A table in the Fibre Channel Standard equates the loop position to the default ALPA.

arbitrated loop

A Fibre Channel topology. The basic definition is a ring of ports where the transmit output of one port is attached to the receive input of the next. Each port has a unique loop address and it talks to other ports on the loop by arbitrating for loop access. Loop addresses are assigned via cooperative port intercommunication during loop initialization, which occurs any time the device configuration on the loop is physically changed. PLDA (private loop direct attach), the specific profile implemented by the controller, is a subset of arbitrated loop.

See also PL_DA or PLDA.

array controller

See controller.

array controller software (ACS)

Software that is contained on a removable PCMCIA program card that provides the operating environment for the array controller.

association sets

An association set is a group of remote copy sets that share common attributes. Members of an association set are configured to transition to the same state at the same time. An association set:

- Shares the same log unit
- Has its host access removed from all members when one member fails
- Keeps I/O order across all members
- Fails over to the alternate controller in the event of primary controller failure.

CLI commands available are ADD ASSOCIATIONS and SET associations.

asynchronous mode

A mode of operation of the remote copy set whereby the write operation provides command completion to the host after the data is safe on the initiating controller, and prior to the completion of the target command.

Asynchronous mode can provide faster response time, but the data on all members at any one point in time cannot be assumed to be identical.

See also synchronous mode.

ATM

Asynchronous Transfer Mode. ATM refers to a network or communications technology used in LANs and WANs to enable disparate traffic (data, voice, and video) to be carried over the same Local or Wide Area Network. ATM is the transfer mode of choice for broadband integrated services digital networks (BISDNs). ATM traffic carries information in fixed-size cells.

autospare

A controller feature that automatically replaces a failed disk drive with a working drive. The operator can enable the AUTOSPARE switch for the failedset, causing physically replaced disk drives to be automatically placed into the spareset. Data recovery is outside the scope of autosparing. Also called *autonewspare*.

bad block

A disk drive data block that contains a physical defect.

bad block replacement

A replacement routine that substitutes defect-free disk blocks for those found to have defects. This process takes place in the controller, transparent to the host.

BBR

See bad block replacement.

block

A stream of data stored on disk or tape media and transferred and error-checked as a unit. In a disk drive, a block is also called a sector (the smallest collection of consecutive bytes addressable on a disk drive). In Compaq integrated storage elements, a block contains 512 bytes of data, error codes, flags, and the block address header.

cache

A fast, temporary storage buffer in a controller or computer.

cache memory

portion of high-speed memory used as an intermediary between a data user and a larger amount of storage. The objective of designing cache into a system is to improve performance by placing the most frequently used data in the highest performance memory and close to the process needing that data.

CBR

An acronym for Constant Bit Rate, a category of ATM service. This category supports a constant (guaranteed) data rate. CBR supports applications that require a highly predictable transmission rate.

cascaded switch

As applied to the Data Replication Manager: the term cascaded switch identifies that the output of a switch is connected to the input of another switch, which then may in turn be connected to another switch or host or controller.

chunk

A block of data written by the host.

See also block, chunk size.

chunk size

The number of data blocks, assigned by a system administrator, written to the primary RAIDset or stripeset member before the remaining data blocks are written to the next RAIDset or stripeset member.

CLI

An acronym for the Command Line Interpreter. Also known as Command Line Interface. The CLI is the configuration interface to operate the controller software.

clone

A utility that physically duplicates data on any unpartitioned single-disk unit, stripeset, mirrorset, or striped mirrorset.

command line interface

or

command line interpreter

See CLI.

connection

As applied to the Data Replication Manager: this refers to a connection between two end Fibre Channel ports. An example would be the connection between a Host Bus Adapter (by way of the Fibre Channel Switches) and the HSG80 controller.

CLI commands available on the HSG80 are ADD CONNECTIONS, SET connection-name.

See also link.

container

1. Any entity that is capable of storing data, whether it is a physical device or a group of physical devices.
2. A virtual internal controller structure representing either a single disk or a group of disk drives linked as a storageset. Examples of storageset containers that the controller uses to create units include stripesets and mirrorsets.

controller

A hardware device that uses software to facilitate communications between a host and one or more storage devices organized in an array. The HS-series *StorageWorks*™ family of controllers are all array controllers.

copying member

In a mirrorset, a copying member is a container introduced to the mirrorset after the mirrorset has already been in use. None of the blocks can be guaranteed to be the same as other members of the mirrorset. Therefore the *copying* member is made the same by copying all the data from a *normal* member. This is in contrast to *normalization*, where all blocks written since creation are known to be the same.

When all of the blocks on the copying member are the same as those on the normal member, the copying member becomes a normal member. Until it becomes a normal member, the copying member contains undefined data and is not useful for any purpose.

DataSafe

Also known as firewall for Microsoft Windows 2000 and NT. This pre-tested configuration uses specific hardware, Data Replication Manager software, and installation practices to protect operations from hardware or software outages. The solution includes No Single Point of Failure (NSPOF) functionality.

default gateway

The default path that a computer or router uses to forward and route data between two or more networks having different protocols.

device

See node, peripheral device.

disaster tolerance

As applied to DRM, disaster tolerance provides the ability for rapid recovery of user data from a remote location when a significant event or a disaster occurs at the primary computing site.

See also remote copy sets, DT.

DT

An acronym for disaster tolerance.

See disaster tolerance.

dual-redundant configuration

A storage subsystem configuration consisting of two active controllers operating as a single controller. If one controller fails, the other controller assumes control of the failing controller's devices.

See also failover, failback.

ECB

An acronym for external cache battery.

See external cache battery.

EMU

Environmental Monitoring Unit. A device that provides increased protection against catastrophic failures. Some subsystem enclosures include an EMU, which works with the controller to detect conditions such as failed power supplies, failed blowers, elevated temperatures, and external air sense faults. The EMU also controls certain rack hardware, including alarms, fan speeds, and certain chips.

environmental monitoring unit

A piece of hardware that provides increased protection against catastrophic failures. Some subsystem enclosures include an EMU, which works with the controller to detect conditions such as failed power supplies, failed blowers, elevated temperatures, and external air sense faults. The EMU also controls certain rack hardware, including DOC chips, alarms, and fan speeds.

external cache battery

The unit that supplies backup power to the cache module in the event the primary power source fails or is interrupted.

F_port

A port in a fabric where an N_Port or NL_Port may attach.

fabric

A network of Fibre Channel switches or hubs and other devices.

failback

The process of restoring data access to the newly-restored controller in a dual-redundant controller configuration. The failback method (full copy or fast failback) is determined by the enabling of the Logging or Failsafe switches, the selected mode of operation (synchronous or asynchronous), and whether the failover is planned or unplanned.

See also failover, dual-redundant configuration.

failedset

A group of disk drives that have been removed from RAIDsets due to a failure or a manual action. Disk drives in the failedset should be considered defective and should be tested and repaired before being placed back into the spareset or back in their original locations.

failover

The process that takes place when storage processing is moved from one pair of controllers at one site to another pair at another site. Failover continues until the processing is failed back to the originator site.

The CLI command is: `SITE_FAILOVER`

See also failback, dual-redundant configuration, planned failover.

failsafe locked

The failsafe error mode can be enabled by the user to fail any write I/O whenever the target is inaccessible or the initiator unit fails. When either of these conditions occurs, the remote copy set goes into the inoperative (offline) state and the failsafe error mode is “failsafe locked.”

The CLI command `SET remote-copy-set-name ERROR_MODE=FAILSAFE` enables this error mode.

fast failback

A term representing the synchronization of the initiator site with the target during a planned failback from the target back to the initiator.

The write operations are logged to the target site write history log, and during the fast failback, the initiator site is updated from the write history log.

See also mini-merge, unplanned failover, planned failover, write history logging.

FC-AL

or

FCAL

An acronym for Fibre Channel Arbitrated Loop. FC-AL is the overall Fibre Channel topology whose basic definition is a ring of ports where the transmit outputs of one port are attached to the receive input of the next. Not supported by DRM.

FC-ATM

An acronym for Fibre Channel Asynchronous Transfer Mode (ATM AAL5 over Fibre Channel). As part of the Fibre Channel Specifications, more information is available from <http://www.t11.org>.

FC-FG

An acronym for Fibre Channel Fabric Generic Requirements. As part of the Fibre Channel Specifications, more information is available from <http://www.t11.org>.

FC-FP

An acronym for Fibre Channel Framing Protocol. As part of the Fibre Channel Specifications, more information is available from <http://www.t11.org>.

See HIPPI-FC.

FC-GS-1

An acronym for Fibre Channel Generic Services-1. As part of the Fibre Channel Specifications, more information is available from <http://www.t11.org>.

FC-GS-2

An acronym for Fibre Channel Generic Services-2. As part of the Fibre Channel Specifications, more information is available from <http://www.t11.org>.

FC-IG

An acronym for Fibre Channel Implementation Guide. As part of the Fibre Channel Specifications, more information is available from <http://www.t11.org>.

FC-LE

An acronym for Fibre Channel Link Encapsulation (ISO 8802.2). As part of the Fibre Channel Specifications, more information is available from <http://www.t11.org>.

FC-PH

An acronym for the Fibre Channel Physical and Signaling Standard.

FC-SB

An acronym for the Fibre Channel Single Byte Command Code Set. As part of the Fibre Channel Specifications, more information is available from <http://www.t11.org>.

FC-SW

An acronym for the Fibre Channel Switched Topology and Switch Controls. This topology involves a structure whose fabric is unknown to the end nodes. The fabric may contain multiple paths between source and destination. As part of the Fibre Channel Specifications, more information is available from <http://www.t11.org>.

FCC

An acronym for the Federal Communications Commission. The federal agency responsible for establishing standards and approving electronic devices within the United States.

FCC Class A

This certification label appears on electronic devices that can only be used in a commercial environment within the United States.

FCC Class B

This certification label appears on electronic devices that can be used in either a home or a commercial environment within the United States.

FCP

An acronym for Fibre Channel Protocol. The mapping of SCSI-3 operations to Fibre Channel.

FDDI

An acronym for Fiber Distributed Data Interface. An ANSI standard for 100 megabaud transmission over fiber optic cable.

FD SCSI

The fast, narrow, differential SCSI bus with an 8-bit data transfer rate of 10 MB/s.

See FWD SCSI and SCSI. More information is available from <http://www.t10.org>.

fiber

An optical strand used in fiber optic cable. Spelled fibre when used in “Fibre Channel” protocol.

See also fiber optic cable, Fibre Channel.

fiber optic cable

A transmission medium designed to transmit digital signals in the form of pulses of light. Fiber optic cable is noted for its properties of electrical isolation and resistance to electrostatic contamination. Available in three sizes: 50-micron multi-mode, 9-micron single-mode, and, in older installations, 62.5-micron multi-mode (not recommended for new installations).

Fibre Channel

An ANSI standard name given to a low-level protocol for a type of serial transmission. The Fibre Channel specifications define the physical link, the low level protocol, and all other pertinent characteristics.

FL_port

A port in a fabric where N_port or an NL_port may be connected.

See N_port, NL_port, F_Port.

See also fabric.

firewall

A generic term used to describe a limited DRM configuration consisting of only two switches. The maximum distance between any two components is 500 meters due to the short range GBICs.

See also DataSafe.

frame

A frame is the basic unit of communication using the Fibre Channel protocol. Each frame consists of a payload encapsulated in control information. The initiator breaks up the exchange into one or more sequences, which in turn are broken into one or more frames. The responder recombines the frames into sequences and exchanges.

See also initiator.

FWD SCSI

Acronym for fast, wide, differential (FWD) Small Computer System Interface (SCSI) bus with a 16-bit data transfer rate of up to 20 MB/sec.

See also FD SCSI and SCSI.

GBIC

An acronym for Gigabit Interface Converter. The hardware devices inserted into the ports of the Fibre Channel switch that hold the Fibre Channel cables. A GBIC converts fiber optic cable connections to Fibre Channel switch connections.

GBICs are available in three types: short wave, long wave, and very long distance. Short wave is limited to 50-micron multi-mode cable and 500 meters. Long wave uses 9-micron single-mode cable and is limited to a maximum distance of 10 kilometers. Very long distance also uses 9-micron low-loss cable and may extend to 100 kilometers.

GLM

Gigabit Link Module, used in short wave multi-mode fiber only. GLMs, as a function of GBIC, are used in Fibre Channel long-distance applications. As applied to the Data Replication Manager, the GLMs provide the ability to increase the fiber optic cable transmission distances from 10 km to 70 km.

hard address

The AL_PA or ALPA which an NL_port attempts to acquire during loop initialization. Not used by DRM.

heterogeneous host support

Also called noncooperating host support. The ability to share storage between two similar (or dissimilar) hosts by way of storage partitioning.

HIPPI-FC

An acronym for the high-performance parallel interface (HIPPI) over the Fibre Channel. HIPPI is a media-level, point-to-point, 12 channel, full-duplex, electrical/optical interface. Not supported by DRM. See <http://www.t11.org> for more information.

hop

The definition of an inter-switch connection. For example, there is one hop between two cascaded switches.

ISL

Intersite link or Interswitch link. The abbreviation is context sensitive.

See also multiple intersite links.

initiator

1. A SCSI device that requests an I/O process to be performed by another SCSI device, namely, the SCSI target. The controller is the initiator on the device bus.
2. For subsystems using the disaster tolerance Data Replication Manager solution, the initiator is the site that is the primary source of information. In the event of a system outage, the data would be recovered from the target system.

See also target.

IP address

An abbreviation for Internet Protocol Address. The IP address is a number that is used as the address specifying a particular computer connected to the internet.

latency

The amount of time required for a transmission to reach its destination.

LBN

An acronym for logical block number.

See logical block number.

L_port

A node or fabric port capable of performing arbitrated loop functions and protocols. NL_port and FL_Port are loop-capable ports.

link

A physical connection between two adjacent Fibre Channel ports, consisting of a transmit fiber and a receive fiber. An example would be the connection between the Fibre Channel switch port and the HSG80 controller.

See also connection.

local terminal

A terminal plugged into the EIA-423 maintenance port on the front bezel of the HS array controller. Also called a maintenance terminal.

Logical Block Number

A volume-relative address of a block on a mass storage device. The blocks that form the volume are labeled sequentially starting with LBN 0.

logical unit

A physical or virtual device addressable through a target ID number. The logical unit numbers (LUNs) use their target's bus connection to communicate on the SCSI bus.

See LUN.

Logical Unit Number

A value that identifies a specific logical unit belonging to a SCSI target ID number. A number associated with a physical device unit during a task's I/O operations. Each task in the system must establish its own correspondence between logical unit numbers and physical devices.

LOG_UNIT

A CLI command switch that (when enabled) assigns a single, dedicated log unit for a particular association set. The association set members must all be in the NORMAL error mode (not failsafe).

See also write history logging.

long distance mirroring

Also known as peer-to-peer remote copy. *See also* remote copy sets.

loop

See also arbitrated loop.

loop_ID

A seven-bit value numbered contiguously from zero to 126-decimal, which represents the 127 legal AL_PA or ALPA values on a loop (not all of the 256 hex values are allowed as AL_PA values per FC-AL).

loop tenancy

The period of time between the following two events: when a port wins loop arbitration and when the port returns to a monitoring state.

L_port

A node or fabric port capable of performing arbitrated loop functions and protocols. NL_Ports and FL_Ports are loop-capable ports.

LUN

An acronym for logical unit number.

See logical unit number.

mini-merge

As applied to the Data Replication Manager: a term representing the data transfers to be made from the write history log when the target becomes available after having been unavailable. This happens when both links or both target controllers have gone down. The transfers that would have been made are instead logged into the association set's assigned log unit to wait until the remote copy set subsystem comes back online.

See fast failback, write history logging.

mirroring

The act of continuously creating an exact physical copy or image of data.

mirrorset

1. A group of storage devices organized as duplicate copies of each other. Mirrorsets provide the highest level of data availability at the highest cost. Another name for RAID 1. Also called mirrored units or mirrored virtual disks.
2. Two or more physical disks configured to present one highly reliable virtual unit to the host.
3. A virtual disk drive consisting of multiple physical disk drives, each of which contains a complete and independent copy of the entire virtual disk's data.

multiple intersite links

Each intersite link (ILS) is a fiber link between two switches. As applied to Data Replication Manager: increasing bandwidth between switches is handled by adding additional connections between the switches, to a maximum of two connections.

N_port

A port attached to a node for use with point-to-point topology or fabric topology.

See point-to-point connection.

NL_port

A port attached to a node for use in all three Fibre Channel topologies: point-to-point, arbitrated loop, and switched fabric.

network

In data communication, a configuration in which two or more terminals or devices are connected to enable information transfer.

node

1. In data communications, the point at which one or more functional units connect transmission lines.
2. In Fibre Channel, a device that has at least one N_port or NL_port.

Non-L_port

A node or fabric port that is not capable of performing the arbitrated loop functions and protocols. N_Ports and F_Ports are loop-capable ports.

non-participating mode

A mode within an L_Port that inhibits the port from participating in loop activities. L_Ports in this mode continue to retransmit received transmission words but are not permitted to arbitrate or originate frames. An L_Port in non-participating mode may or may not have an AL_PA.

See also participating mode.

non-RCS LUN

As applied to Data Replication Manager: a logical unit number (LUN) value that identifies a physical device unit which exists at one of the two sites and does not have a mirror copy at the other site.

See also remote copy sets, LUN.

normal member

A mirrorset member that, block-for-block, contains exactly the same data as that on the other members within the mirrorset. Read requests from the host are always satisfied by normal members.

normalizing

A state in which, block-for-block, data written by the host to a mirrorset member is consistent with the data on other normal and normalizing members. The normalizing state exists only after a mirrorset is initialized. Therefore, no customer data is on the mirrorset.

normalizing member

A mirrorset member whose contents are the same as all other normal and normalizing members for data that has been written since the mirrorset was created or since lost cache data was cleared. A normalizing member is created by a normal member when either all of the normal members fail or all of the normal members are removed from the mirrorset.

See also copying member

OC-3

An acronym for the optical carrier that provides high-speed bandwidth at 155.3 megabits per second.

other controller

The controller in a dual-redundant pair that is not connected to the controller serving your current CLI session with a local terminal.

See also this controller, local terminal.

participating mode

A mode within an L_port that allows the port to participate in loop activities. A port must have a valid AL_PA or ALPA to be in participating mode.

PCM

An acronym for Polycenter Console Manager.

PCMCIA

An acronym for Personal Computer Memory Card Industry Association. An international association formed to promote a common standard for PC card-based peripherals to be plugged into notebook computers. A PCMCIA card, sometimes called a PC Card, is about the size of a credit card. It is used in the HSG80 to load the controller software.

See also program card, ACS.

PCR

An acronym for peak cell rate, the maximum transmission speed of a virtual connection. PCR is a required parameter for the CBR service category.

peer-to-peer remote copy

See remote copy sets.

peripheral device

Any unit, distinct from the CPU and physical memory, that can provide the system with input or accept any output from it. Terminals, printers, tape drives, and disks are peripheral devices.

planned failover

As applied to the Data Replication Manager: an orderly shutdown of the initiator site applications and controllers for installation of new hardware, updating the software, and so on. The host applications are quiesced and all write operations permitted to complete before the shutdown. The controllers must be in synchronous operation mode before starting a planned failover.

See also synchronous mode, unplanned failover.

PL_DA

or

PLDA

An acronym for Private Loop Direct Attach. PLDA is a Fibre Channel profile, a proper subset of arbitrated loop. The PLDA profile (part of the Fibre Channel Standard), defines a specific way to implement arbitrated loop topology. Not supported by DRM.

See arbitrated loop.

point-to-point connection

A network configuration in which a connection is established between two, and only two, terminal installations. The connection may include switching facilities.

See N_port.

port

- In general terms, a port is:
 1. A logical channel in a communications system.
 2. The hardware and software used to connect a host controller to a communications bus, such as a SCSI bus or serial bus.
- Regarding the controller, the port is:
 1. The logical route for data in and out of a controller that can contain one or more channels, all of which contain the same type of data.
 2. The hardware and software that connect a controller to a SCSI device.

port_name

A 64-bit unique identifier assigned to each Fibre Channel port. The Port_Name is communicated during the logon and port discovery process.

preferred address

The AL_PA which an NL_Port attempts to acquire first during initialization.

private NL_port

An NL_Port which does not attempt login with the fabric and only communicates with NL_Ports on the same loop. Not used by DRM.

public NL_port

An NL_port that attempts login with the fabric and can observe the rules of either public or private loop behavior. A public NL_Port may communicate with both private and public NL_Ports. Not used by DRM.

program card

The PCMCIA card containing the controller's operating software.

See also PCMCIA.

PTL

An acronym for Port-Target-LUN. The controller's method of locating a device on the controller device bus:

- P designates the port (1—6)
- T designates the target ID of the device (1—6 in a non-redundant configuration, or 0—5 in a dual-redundant configuration)
- L designates the LUN of the devices (0—7).

PVA module

An abbreviation for Power Verification and Addressing module. The Ultra SCSI RAID enclosure assembly whose primary functions are to: (1) allow the user to select the enclosure Ultra SCSI bus ID; (2) enable the user to place the subsystem in a standby condition and return it to an operational status; and (3), in conjunction with the associated EMU, ensures that the major Ultra SCSI elements are functioning properly and notifies the user and the controller of error or fault conditions.

PVC

An acronym for Permanent Virtual Circuit. PVC is a logical connection manually defined by the network administrator. The PVC is created by specifying the VPI and VCI.

quiesce

To make a bus inactive or dormant. In a DRM environment, quiesce means to shut down or freeze applications such that all pending I/O is completed and no new I/O is initiated by the application until a thaw or unquiesce command is issued. During a device warm swap, the SCSI bus must quiesce.

See also planned failover.

QoS

An acronym for Quality of Service in an ATM network. Each virtual connection in an ATM network is set to a service category. The performance of the connection is measured by the established QoS parameters (outlined by the ATM Forum).

Performance issues include data rate, cell loss rate, cell delay, and delay variation (jitter).

Categories of ATM service are:

- Constant Bit Rate (CBR)
- Variable Bit Rate-Real Time (VBR-RT)
- Variable Bit rate- Non-Real Time (VBR-NRT)
- Available Bit Rate (ABR)
- Unspecified Bit Rate (UBR)

See ATM.

RCS

See remote copy sets.

redundancy

The provision of multiple interchangeable components to perform a single function in order to cope with failures and errors. A RAIDset is considered to be redundant when user data is recorded directly to one member, and all of the other members and associated parity also are recorded. If a member is missing from the RAIDset, its data can be regenerated as needed, but the RAIDset is no longer redundant until the missing member is replaced and reconstructed.

remote copy sets

A feature that allows data to be copied (mirrored) from the originating site (initiator) to a remote site (target). The result is a mirror copy of the data (remote copy set) at two disparate sites. Used in disaster tolerance (DT) applications such as the Data Replication Manager.

CLI commands available are: ADD REMOTE_COPY_SETS, SET remote-copy-set-name, SET controller REMOTE_COPY.

See also disaster tolerance, non-RCS LUN.

remote copy set metadata

Remote copy set metadata describes the remote copy set membership and state. To assist with site failover, this metadata is located in the mirrored write-back cache on the controller where each member resides. Backup copies of the metadata reside in the controller NVRAM at each site. Only the initiator modifies the metadata and ensures all copies are subsequently updated.

replacement policy

The policy specified by a CLI command switch (SET FAILEDSET command) indicating whether a failed disk from a mirrorset or RAIDset is to be automatically replaced with a disk from the spareset. The two switch choices are AUTOSPARE and NOAUTOSPARE.

SCSI

An acronym for Small Computer System Interface:

1. An American National Standards Institute (ANSI) interface standard defining the physical and electrical parameters of a parallel I/O bus used to connect initiators to devices.
2. A processor-independent standard protocol for system-level interfacing between a computer and intelligent devices, including hard drives, floppy disks, CD-ROMs, printers, scanners, and others.

Refer to <http://www.t10.org> for more information.

SCSI device

1. A host computer adapter, a peripheral controller, or an intelligent peripheral that can be attached to the SCSI bus.
2. Any physical unit that can communicate on a SCSI bus.

SCSI device ID number

A bit-significant representation of the SCSI address referring to one of the signal lines, numbered 0 through 7 for an 8-bit bus, or 0 through 15 for a 16-bit bus.

SCSI ID number

The representation of the SCSI address that refers to one of the signal lines numbered 0 through 15.

snapshot

A snapshot unit is one that reflects the contents of another unit at a particular point in time. It is a virtual copy and not a physical copy of the source device at a point in time.

See also unit.

storage array

An integrated set of storage devices. Storage arrays can be manipulated as one unit.

storage unit

The general term that refers to storagesets, single-disk units, and all other storage devices that are installed in a subsystem and accessed by the host. A storage unit can be any entity that is capable of storing data, whether it is a physical device or a group of physical devices.

storageset

1. A group of devices configured with RAID techniques to operate as a single container.
2. Any collection of containers, such as stripesets, mirrorsets, striped mirrorsets, JBODs, and RAIDsets.

subnet mask

Also known as address mask. A subnet is an IP network that can be reached through a single IP address. All the members of the subnet share the mask value. Members of the subnet can then be referenced more easily. A subnetwork is a network that is part of another network, connected through a gateway, bridge, or router.

surviving controller

The controller in a dual-redundant configuration pair that serves its companion's devices when the companion controller fails.

SWCC

An acronym for Storage Works Command Console.

synchronous mode

A mode of operation of the remote copy set whereby the data is written simultaneously to the cache of the initiator subsystem and the cache of the target subsystem. The I/O completion status is not sent until all members of the remote copy set are updated.

See also asynchronous mode.

target

A SCSI device that performs an operation requested by another SCSI device, namely the SCSI initiator. The target number is determined by the device's address on its SCSI bus.

For subsystems using the disaster-tolerant Data Replication Manager solution, data processing occurs at the initiator site and the data is replicated or mirrored to the target site. In the event of a system outage, the data would be recovered from the target system.

See also initiator.

this controller

The controller that is serving the current CLI session through a local or remote terminal.

See also other controller.

UBR

An acronym for unspecified bit rate. The UBR is a category of ATM service that supports connections that have no specified performance requirements.

ULP

An acronym for Upper Layer Protocol.

ULP process

A function executing within a Fibre Channel node which conforms to the Upper Layer Protocol (ULP) requirements when interacting with other ULP processes.

UltraNet Wizard

Another term for the Fibre Channel-to-ATM Configuration Wizard. This wizard is an UltraNet application that allows the designation of the default configuration settings for Fibre-Channel-ATM on the Open Systems Gateway.

unit

A container made accessible to a host. A unit may be created from a single disk drive or tape drive. A unit may also be created from a more complex container, such as a RAIDset. The controller supports a maximum of eight units on each target.

unplanned failover

As applied to the Data Replication Manager: an unplanned outage of the initiator site controllers. This may occur when the site communication is lost, or due to some other failure whereby remote copy sets cannot be implemented. The controllers do not perform an orderly shutdown.

See also planned failover.

VCI

An acronym for virtual channel identifier. The VCI is the field of the ATM cell header that stores the virtual channel address.

VPI

An acronym for virtual path identifier. The VCI is the field of the ATM cell header that stores the virtual path address.

World Wide Name

or

World wide ID

Also known by the acronym WWN. A unique 64-bit number assigned to a subsystem by the Institute of Electrical and Electronics Engineers (IEEE) and set by manufacturing prior to shipping. This name is referred to as the node ID within the CLI.

write history logging

As applied to the Data Replication Manager: the use of a log unit to log a history of write commands and data from the host. Write history logging is used for mini-merge and fast-failback.

See mini-merge, fast failback.

WTI Switch

An abbreviation for the Western Telematic Switch that must be installed to set up and service the ATM gateway. The WTI switch is a 16-port serial switch that is used to configure or service the OSG unit locally or remotely.

zone

A set of devices that access one another. All devices connected to a fabric may be configured into one or more zones. Devices that are in the same zone can see each other; devices that are in different zones cannot.

zone alias

Zone aliases simplify the entry of repetitive port numbers or World Wide Names. A zone alias is a C-style name for one or more port numbers or World Wide Names (e.g., the named host could be used as an alias for 10:00:00:60:69:00:00:8a).

zone configuration

A set of zones. At any one time zoning may be disabled or one zone configuration may be in effect. When a zone configuration is in effect, all zones that are members of that configuration are in effect. You select which zone configuration is currently in effect.

zoning

As applied to the Data Replication Manager: an optionally licensed feature of Compaq SAN switches that allows a finer segmentation of Storage Area Networks (SANs) by allowing ports or WWN addresses to be used to confine access to devices that are in a common zone.

Index

!NEWCONxx connections

renaming to previous names 9–38

A

adding back initiator unit to remote copy sets at initiator site 3–4, 4–4, 8–5

adding back initiator unit to remote copy sets at target site 2–18, 7–18, 9–29

adding new unit protected by new remote copy set 9–9

allowing hosts to recognize new units at initiator site 2–28, 9–41

allowing hosts to recognize new units at target site 2–8, 5–16, 7–13, 9–10, 10–13

allowing write history log to merge 5–20

application action list 1–12

applications names, convention defined xii

assigning log unit to association set 5–12, 6–4, C–3

association sets

creating 5–11, 6–4, C–2

deleting at initiator site 2–16, 5–4, 6–9, 7–4, 10–4

deleting at target site 5–21, 9–35

asynchronous operation mode 2–18, 2–25, 5–4, 5–24, 7–4, 7–18, 7–21, 7–26, 9–37, 10–4, 10–9, 11–9

asynchronous transfer mode 1–2

audience ix

authorized reseller, Compaq xv

B

beginning a failback or failover too soon 1–4

breaking connection between sites 2–2

bus

Fibre Channel 1–13

button names, convention defined xii

C

caution, symbol and definition xii

changing from asynchronous to synchronous mode at initiator site 5–4, 7–4, 10–4

changing from asynchronous to synchronous mode at target site 7–21

changing from synchronous to asynchronous mode at initiator site 2–25, 5–24, 7–26, 9–37, 11–9

changing from synchronous to asynchronous mode at target site 2–18, 7–18, 10–9

checksum

location 9–14

setting 9–14

clearing lost data at initiator site 2–12, 7–16, 11–7

COM port A–1

command line interpreter (CLI) commands

using in case of scripting problems 1–12

command names, convention defined xii

Command Scriptor 1–12, 1–13

Compaq

authorized reseller xv

technical support xiv

website xv

component

failures 12–4

repair vs. failover 1–4

configuration file 1–12

connection to fabric

- restoring connection from initiator site 11–6
- connections
 - remote copy set 7–4, 10–4
 - restoring to target site 2–17, 2–24, 5–8, 7–9, 7–24, 9–36, 10–8
- connections to original controllers
 - deleting at initiator site 9–23
- control table 1–13
- controller
 - failure of one dual redundant member 12–5
 - forced errors during copy 12–2
 - operating characteristics 12–2
 - read errors during copy 12–2
- controller access
 - disconnecting at initiator site 2–21, 7–21, 9–31, 11–2
 - disconnecting at target site 5–7, 7–7, 9–3, 10–7, 11–6
- controller failover vs. site failover 1–4
- controller prompt
 - designating 9–16
- conventions
 - application names, defined xii
 - button names, defined xii
 - command names, defined xii
 - dialog box names, defined xii
 - document xii
 - file names, defined xii
 - keyboard keys, defined xii
 - menu items, defined xii
 - menu sequences, defined xii
 - system responses, defined xii
 - user input, defined xii
 - variables xii
 - website addresses xii
- creating a log unit 5–9, C–1
- creating a mirrorset 5–9, 6–2, C–1
- creating association sets 5–11, 6–4, C–2

D

- data
 - mirrored 1–2
- Data Replication Manager
 - basic configuration diagram 1–3
 - component failures 12–4
 - overview 1–2
- deleting association sets at initiator site 2–16, 5–4, 6–9, 7–4, 10–4
- deleting association sets at target site 5–21, 9–35
- deleting connections to original controllers at initiator site 9–23
- deleting remote copy sets at initiator site 2–16, 7–17, 11–3
- deleting remote copy sets at target site 2–22, 7–23, 9–35, 11–6
- designating controller prompt 9–16
- determining which controller the remote copy set LUN is online to 4–2
- dialog box names, convention defined xii
- disabling host access to remote copy set units at initiator site 2–15, 5–4, 7–4, 9–18, 10–4
- disabling host access to remote copy set units at target site 2–20, 5–20, 7–20, 9–30, 10–17, 11–6
- disabling initiator controller access to remote copy sets at target site 9–22
- disabling node access to log unit C–3
- disabling node access to log unit at initiator site 6–3
- disabling node access to log unit at target site 5–11
- disabling write history logging at target site 2–22, 5–20, 7–23, 9–34, 10–17
- disabling writeback cache C–3
- disabling writeback cache at initiator site 6–3
- disabling writeback cache at target site 5–11
- disaster tolerance
 - failure modes in normal operation 12–6
- disaster tolerant (DT) 1–2
 - failure notification 12–4
- disaster-tolerant (DT) 12–4

- disconnecting controller access at initiator site 2–21, 7–21, 9–31, 11–2
- disconnecting controller access at target site 5–7, 7–7, 9–3, 10–7, 11–6
- document
 - conventions xii
 - prerequisites xii
- documentation, related x
- DRM hardware 1–7
- DRM Scripting Kit 1–12
- dual redundancy
 - failure of one member 12–5
- dual-link failure 12–3
- E**
- electrical shock hazard, symbol and definition xiii
- enabling access from initiator host to storage units 11–3
- enabling access to initiator site host 10–20
- enabling access to original initiator site host 5–24
- enabling host access to remote copy set units at initiator site 9–40
- enabling host access to remote copy set units at target site 2–6, 5–13, 7–11, 9–6, 10–11
- enabling host access to remote copy units at initiator site 2–26, 7–27
- enabling initiator controller access to remote copy set units at target site 9–28
- enabling port 1 & 2 connections to fabric 9–20
- enabling remote copy set unit access to target site controllers 5–5
- enabling target controller access to remote copy set units at initiator site 9–27
- equipment symbols xiii
- error messages
 - error-initiator unit specified not found* 9–26
 - error-initiator unit specified not found. 9–25
- Error_Mode = Failsafe 1–5
- Error_Mode = Normal 1–5
- establishing connection to target site 9–26
- establishing connections to initiator site 9–25
- event log 2–1
- excessive weight, symbol and definition xiv
- extended duration site maintenance 1–8
- extended planned loss
 - resumption of replication 1–8
- F**
- failback
 - dual redundancy 12–2
 - full 1–7
 - resuming 2–19, 9–30
- failing back initiator role to initiator site 7–22
- failing over remote copy sets 2–4, 9–5
- failover
 - failure at target site after failover 12–7
 - planned failover 5–2, 11–1
 - unplanned 1–4, 1–7, 1–9, 2–2
 - unplanned with full failback 2–1
 - when to 1–4
- failover and failback 1–3
- failover event
 - loss of intersite connections 1–9
- failover scenarios 1–6
- failover vs. component repair 1–4
- failsafe
 - failsafe lock management 12–3
- failsafe mode
 - remote copy sets 12–3
 - setting at initiator site 2–25, 3–6, 5–24, 7–26, 9–38, 11–10
 - setting at target site 2–19
- failsafe-locked mode 1–6
- failures
 - at target site after failover 12–7
 - component 12–4
 - dual-link 12–3
 - network 12–6
 - notification 12–4
 - StorageWorks Command Console 12–5
 - types 1–5
- fast failback
 - after planned site failover 5–19

- initiator site cleanup 5–22
- target site failback 5–20
- Fibre Channel bus 1–13
- Fibre Channel switches 1–2
- file names, convention defined xii
- forced errors 12–2
- full failback
 - after unplanned site failover 1–7
 - initiator site preparation 2–12, 7–16
 - initiator site restoration of target connections 2–24, 7–24
 - initiator site return control 2–21, 7–21
 - target site copy data 2–17, 7–18, 7–20
 - target site restore 2–22, 7–23
- full normalization vs. merge 5–10, C–1
- G**
- getting help xiv
 - Compaq technical support xiv
 - Compaq website xv
- GUI.ini file 12–5
- H**
- hardware
 - DRM 1–7
 - redundancy 1–2
- help, obtaining xiv
- host access to to remote copy units
 - enabling at initiator site 2–26, 7–27, 9–40
- host I/O
 - resuming at initiator site 3–3
- hot surface, symbol and definition xiii
- hyphens in naming convention 1–13
- I**
- I/O performance at initiator site
 - enhancing 5–22, 10–18
- I/O performance at target site
 - enhancing 2–7, 5–12, 7–11, 9–8, 9–40, 10–10
- important, defined xii
- initializing a mirrorset 5–10, 6–3, C–1
- initiator controller access
 - disabling access to at target site 9–22
- initiator controllers
 - shutting down 7–6
- initiator host name
 - recalling 2–15
- initiator role
 - failing back to initiator site 7–22
 - moving to target controller 5–8
 - moving to target site 7–8, 10–8
- initiator site
 - establishing connections to 9–25
 - failure modes in normal operation 12–6
- initiator site cleanup 5–22, 11–6
- initiator site connections 9–26
- initiator site host
 - enabling access to 10–20
- initiator site preparation 2–12, 5–2, 7–2, 7–16, 10–2, 11–2
- initiator site procedure steps identification 2–1
- initiator site restoration of target connections 2–24, 7–24, 9–36
- initiator site return control 2–21, 7–21, 9–31
- initiator unit
 - adding back to remote copy sets at initiator site 3–4, 4–4, 8–5
 - adding back to remote copy sets at target site 2–18, 7–18, 9–29
- initiator vs. target 1–3
- initiators
 - multiple 1–2
- instance code
 - comparing screen with example display 2–1
- K**
- keyboard keys, convention defined xii
- L**
- launch file 1–13
- leaving load running at target site 2–19
- link failure management 12–3
- log disk failure
 - full normalization vs. merge 5–10, C–1
- log unit

- assigning to association set 5-12, 6-4, C-3
- creating 5-9, C-1
- presenting to controller 5-10, 6-3, C-2
- logged data
 - protection 5-10, C-1
- loss of initiator site
 - unplanned 2-1
- loss of intersite connections 1-9
- loss of target
 - unplanned 1-7
- lost data
 - clearing at initiator site 2-12, 7-16, 11-7

M

- maintenance completion 7-16
- maintenance failback 7-20
- maximum cached transfer size
 - setting 10-18
 - setting at initiator site 2-16, 2-27, 5-5, 5-22, 7-5, 7-28, 9-20, 10-5, 10-18
 - setting at target site 2-7, 2-23, 5-12, 5-21, 7-11, 7-23, 9-8, 9-35, 9-40, 10-10
- menu
 - items, convention defined xii
 - sequences, convention defined xii
- mirroring of data 1-2
- mirrorset
 - creating 5-9, 6-2, C-1
 - initializing 5-10, 6-3, C-1
 - one-member 5-10, C-1
- moving initiator role to target controller 5-8
- moving initiator role to target site 7-8, 10-8
- moving initiator role to the original initiator 2-22, 9-33
- moving remote copy sets control to original initiator 5-21
- multi-host environment
 - failure 1-6
- multiple initiator subsystems 1-2
- multiple power source, symbol and definition xiii

N

- naming convention
 - use of hyphens 1-13
- network interface connection, symbol and definition xiii
- new hardware failback 9-13
 - initiator site connections 9-26
 - initiator site preparation 9-13
 - initiator site restoration of target connections 9-36
 - initiator site return control 9-31
 - target site copy data 9-28
 - target site preparation 9-22
 - target site restore 9-34
- new unit protected by new remote copy set
 - adding 9-9
- new units
 - allowing hosts to recognize at initiator site 2-28, 9-41
 - allowing hosts to recognize at target site 2-8, 5-16, 7-13, 9-10, 10-13
- node
 - disabling access to at initiator site 6-3
 - disabling access to log unit C-3
 - disabling access to log unit at target site 5-11
- node ID
 - location 9-14
 - setting 9-14
- non-catastrophic failures 1-3
- normal error mode 1-5
- normal mode 1-6
- normalization completion percentage
 - viewing normalization completion percentage
 - at initiator site 3-5, 4-5, 7-19, 8-5, 9-30, 10-10
 - at target site 2-18, 7-18
- note, defined xiii

O

- one-member mirrorset 5-10, C-1
- operating systems

- setting connections back to 9–39
- operating system-specific steps at initiator site
 - 2–13, 2–28, 5–3, 5–24, 7–3, 7–28, 9–13, 9–41, 10–2, 10–20, 11–3
- operating system-specific steps at target site 2–8, 5–16, 7–13, 9–10, 9–41, 10–13
- overview
 - Data Replication Manager 1–2

P

- peer-to-peer remote copy 1–2
- Perl interpreter 1–12, 1–13
- Perl programming language 1–12
- planned failover
 - initiator site preparation 5–2, 7–2
 - maintenance completion 7–16
 - target host setup 5–12, 7–11
 - target site failover 5–6, 7–6
- planned failover vs. unplanned failover 1–4
- planned role reversal 1–9
- port 1 & 2
 - enabling connections to fabric 9–20
- power distribution unit (PDU) B–1
- power down DRM systems B–2
- power up DRM systems B–1
- preferred path
 - setting at initiator site 9–19
 - setting at target site 2–3, 5–6, 7–6, 9–4, 10–6
- preferred SCSI mode
 - setting controller to 9–15
- preparing remote copy sets 8–2
- prerequisites xii
- presenting log unit to controller 5–10, 6–3, C–2
- procedure choices
 - summary 1–9
- protected storage 12–3
- protection of logged data 5–10, C–1

R

- rack stability, warning xiv
- read errors 12–2
- recalling initiator host name 2–15

- recalling target host name 2–6, 5–14, 7–11, 9–7, 10–11
- reconnecting remote controller access 11–6
- recreating remote copy sets at initiator site 11–8
- redundancy
 - hardware 1–2
- re-enabling failsafe mode at initiator site 2–25, 5–24, 7–26, 9–38, 11–10
- related documentation x
- remote controller access
 - reconnecting 11–6
- remote copy set connections 7–4, 10–4
- remote copy set LUN
 - determining which controller it is online to 4–2
 - removing 4–3
- remote copy set unit units
 - connections 5–4
- remote copy set units
 - disabling host access to at initiator site 2–15, 5–4, 7–4, 9–18, 10–4
 - disabling host access to at target site 2–20, 5–20, 7–20, 9–30, 10–17, 11–6
 - enabling access to target site controllers 5–5
 - enabling target controller access to at initiator site 9–27
- remote copy sets
 - asynchronous operation mode 2–18, 2–25, 5–4, 5–24, 7–4, 7–18, 7–21, 7–26, 9–37, 10–4, 10–9, 11–9
 - deleting at initiator site 2–16, 7–17, 11–3
 - deleting at target site 2–22, 7–23, 9–35, 11–6
 - enabling host access at target site 2–6, 5–13, 7–11, 9–6, 10–11
 - enabling initiator controller access at target site 9–28
 - failing over 2–4
 - failsafe mode 12–3
 - member failure 12–3
 - moving control to original initiator 5–21
 - peer-to-peer copy function 1–2

- recreating at initiator site 11–8
 - synchronous operation mode 2–18, 2–25, 5–4, 5–24, 7–4, 7–18, 7–21, 7–26, 9–37, 10–4, 10–9, 11–9
 - worldwide LUN ID 12–4
 - removing remote copy set LUN 4–3
 - removing targets at initiator site 3–3, 8–3
 - removing targets at target site 2–4, 7–9, 9–5
 - renaming !NEWCONxx connections to previous names 9–38
 - restoring connection to fabric from initiator site 11–6
 - restoring connections to target site 2–17, 2–24, 5–8, 7–9, 7–24, 9–36, 10–8
 - resuming failback 2–19, 9–30
 - resuming host I/O at initiator site 3–3
 - resuming operations after loss of target
 - resumption of host access to remote copy sets 3–3, 4–2
 - resumption of operations and return to failsafe mode 3–4
 - verification of lost connections 3–2, 4–2
 - verification of resumption of operations 4–4
 - resuming remote copy sets 6–7
 - resuming write operations to target site 6–7
 - resumption of availability 8–4
 - resumption of host access to remote copy sets 3–3, 4–2
 - resumption of operations and return to failsafe mode 3–4
 - resumption of replication 1–8
 - resumption of replication after extended planned loss of target
 - preparing remote copy sets 8–2
 - resume remote copy set operation 8–4
 - resumption of availability 8–4
 - resumption of replication after short planned loss of target
 - resuming remote copy sets 6–7
 - suspend remote copy sets for target site shutdown 6–2
 - target site shutdown 6–6
 - role reversal
 - planned 1–9
 - recovery from disaster 1–9
 - role reversal failback 10–16
 - initiator site cleanup 10–18
 - target site simple failback 10–16
 - role reversal failover
 - initiator site preparation 10–2
 - target host setup 10–10
 - target site failover 10–6
 - role reversal unplanned failback
 - initiator site cleanup 11–6
 - initiator site preparation 11–2
 - target site cleanup 11–5
- ## S
- Scripting User Guide 1–12
 - scripts
 - available as a procedure 1–10
 - failover and failback 1–12
 - redundancy at initiator and target sites 1–12
 - SCSI mode 9–15
 - setting checksum 9–14
 - setting connections to operating systems 9–39
 - setting controller to preferred SCSI mode 9–15
 - setting error mode of remote copy sets to normal at initiator site 6–2
 - setting error mode to failsafe at initiator site 8–6
 - setting failsafe for units in association set used for write history logging 2–19
 - setting failsafe mode at initiator site 3–6
 - setting failsafe mode at target site 2–19
 - setting maximum cached transfer size 10–18
 - setting maximum cached transfer size at initiator site 2–16, 2–27, 5–5, 7–5, 7–28, 9–20, 10–5
 - setting maximum cached transfer size at target site 2–23, 7–23, 9–35
 - setting node ID 9–14
 - setting port 2 topology offline 2–2
 - setting preferred path at initiator site 9–19

- setting preferred path at target site 2-3, 5-6, 7-6, 9-4, 10-6
 - short duration planned outage at initiator site 5-1
 - short duration site maintenance 1-8
 - short planned loss of target
 - resumption of replication 1-8
 - shutting down initiator controllers 7-6
 - single component failure 1-4
 - site failover 2-22, 9-5, 9-33
 - described 1-4
 - site failover vs. controller failover 1-4
 - site maintenance
 - extended duration 1-8
 - short duration 1-8
 - status comparison
 - target site terminal emulator session A-1
 - storage units
 - enabling access from initiator host 11-3
 - StorageWorks Command Console
 - failure 12-5
 - summary of procedure choices 1-9
 - suspend remote copy sets for target site shutdown 6-2
 - suspending write operations to target site 5-12, 6-5
 - symbol
 - event log 2-1
 - symbol for initiator site steps 2-1
 - symbol for target site steps 2-1
 - symbols
 - in text xii
 - on equipment xiii
 - synchronous operation mode 2-18, 2-25, 5-4, 5-24, 7-4, 7-18, 7-21, 7-26, 9-37, 10-4, 10-9, 11-9
 - system responses, convention defined xii
- T**
- target host name
 - recalling 2-6, 5-14, 7-11, 9-7, 10-11
 - target host setup 5-12, 7-11, 10-10
 - target site
 - establishing connection to 9-26
 - failure after failover 12-7
 - failure modes in normal operation 12-6
 - target site cleanup 11-5
 - target site copy data 2-17, 7-18, 7-20, 9-28
 - target site failback 5-20
 - target site failover 2-2, 5-6, 7-6, 9-2, 10-6
 - target site preparation 9-22
 - target site procedure steps identification 2-1
 - target site restore 2-22, 7-23, 9-34
 - target site shutdown 6-6
 - target site terminal emulator session A-1
 - target sites
 - quantity per initiator site 1-2
 - target vs. initiator 1-3
 - targets
 - removing at initiator site 3-3, 8-3
 - removing at target site 2-4, 7-9, 9-5
 - technical support, Compaq xiv
 - text symbols xii
 - troubleshooting
 - component failures 12-4
 - dual redundancy during failback 12-2
 - failsafe lock management 12-3
 - failure at target site after failover 12-7
 - failure modes in normal operation 12-6
 - failure notification 12-4
 - failure of one dual redundant member 12-5
 - forced errors during copy 12-2
 - link failure management 12-3
 - network failure 12-6
 - read errors during copy 12-2
 - remote copy set failure 12-3
 - remote copy set worldwide LUN ID 12-4
 - StorageWorks Command Console failure 12-5
 - turning off write history logging at initiator site 2-16, 5-4, 6-9, 7-4, 10-4
 - types of failure 1-5

U

unplanned failover 9–2
 target site failover 2–2, 9–2
unplanned failover vs. planned failover 1–4
unplanned loss of initiator 2–1
unplanned loss of target 1–7
unplanned loss of target due to failure of intersite
 links 3–1
unplanned site failover 1–7, 1–9
unplanned site failover with full failback 2–1
user input, convention defined xii

V

variables, convention defined xii
verification of lost connections 3–2, 4–2
verification of resumption of operations 4–4

W

warning
 electrical shock hazard symbol, defined xiii
 excessive weight symbol, defined xiv
 hot surface symbol, defined xiii
 multiple power source symbol, defined xiii
 network interface connection symbol,
 defined xiii
 rack stability xiv

 symbol and definition xii
website addresses, convention defined xii
websites
 Compaq storage xv
 Compaq technical support xiv
when to failover 1–4
world wide LUN ID (WWLID) 12–4
 for remote copy sets 12–4
write history log
 allowing to merge 5–20
write history logging
 disabling at target site 2–22, 5–20, 7–23,
 9–34, 10–17
 turning off at initiator site 2–16, 5–4, 6–9,
 7–4, 10–4
write operations
 suspending to target site 5–12
write operations to target site
 resuming 6–7
 suspending 6–5
writeback cache
 disabling C–3
 disabling at initiator site 6–3
 disabling at target site 5–11

