Compaq Computer Corporation

At Compaq Computer (again!) I created documentation for two Storage Network Products:

- The Compaq Array Controller Software Solution kit enables the user to define, set-up and manage large storage systems.

- Secure Path is a server based software product that provides path management from server to storage system. Its main feature is that it routes I/O from failed path to active or passive paths.

Project Audience

This intended audience for these documents was individuals responsible for installing and configuring Compaq Storage Network products.

Project Specifications

I created the following documents during my contract with Compaq StorageWorks:

- For the Compaq Array Controller Software Solution kit I created 18 Installation Guides and 18 Application Notes for two controllers and nine operating systems. Using FrameMakers' conditionalized text feature, I worked with only two source files (one for each controller) for each document. Each Installation Guide was approximately 200 pages. Each Application Note was approximately 50 pages.

- For Secure Path I created 9 Installation Guides and 9 Application Notes, again using FrameMaker's conditionalized text feature. Each Installation Guide was approximately 100 pages. Each Application Note was approximately 30 pages.

- For Secure Path, I created a documentation plan that contained scheduling and other documentation information for the project.

Personal Responsibilities

I jumped into the Compaq Array Controller Software Solution software project knowing very little about the product. Within a short period of time, I was required to create 36 documents. For accomplishing this feat I was giving an employee excellence award. For the Secure Path project, I was not only responsible for creating the documents, but also attended team leaders meetings and created document schedules (which were constantly being adjusted).

Attached Sample

The attached sample is an overview of the Secure Path technology. It includes features and operation summaries.

1

Secure Path Technology

Compaq *SANworks*^{TM} Secure Path is a server-based software product that enhances
StorageWorks^{TM} RAID Array storage systems by providing automatic path
management from server-to-storage systems during connection failures. Secure Path
supports multiple I/O paths between host and storage, which improves overall data
availability. If any component in a path between host and storage fails, Secure Path
redirects pending and subsequent I/O requests to an alternate path.

This chapter provides the following Secure Path information:

- Features

- Software Components

- Configuration Limitations

- Path Status

- Failover Operation

- Path Management Behavior Summary.

Overview

Compaq SANworks Secure Path for Microsoft Windows is a high-availability
software product that manages and maintains continuous data access to the following
host operating systems:

- Windows NT Server 4.0 and Enterprise Edition

- Windows 2000 Server and Advanced Server

- Windows 2000 Datacenter Advanced Server

SANworks Secure Path for Microsoft Windows provides support for the following
storage systems:

- Enterprise V1.0

- RA/MA8000

- ESA/EMA12000

- MSA1000

- MA6000

Use the SANworks Secure Path software with StorageWorks RAID Arrays configured to operate in any of the following high availability environments:

- Windows NT 4.0 operating systems using Intel-based platforms

- Windows 2000 operating systems using a single host server

- Microsoft Cluster Server (MSCS)

- Oracle Parallel Server (OPS)

Features

Secure Path provides the following features:

- Allows StorageWorks dual-controller RAID systems and host servers equipped with multiple HBA redundant physical connectivity to operate along independent Fibre Channel Arbitrated Loop (FC-AL) or SAN-switched fabric paths.

- Monitors each path and automatically re-routes I/O to a functioning alternate path if an HBA, cable, switch or controller failure occurs.

- Determines the status of physical paths through the implementation of path verification diagnostics.

- Monitors and identifies failed paths and failed-over storage units.

- Automatically restores failed-over storage units to repaired paths with auto-failback capability enabled.

- Continuously monitors and prevents failover/failback ping-pong effects caused by marginal or intermittent conditions.

- Provides a choice of user selectable load balancing algorithms which optimize system workload performance.

- Detects failures reliably without inducing false or unnecessary failovers.

- Implements failover/failback actions transparently without disrupting applications.

- Provides client/server web-based management capability, and multiple storage system support.

Software Components

The Secure Path Software kit for Windows includes the following software components.

- **HszDisk.sys** is a Windows NT class driver that provides unique error handling features and performance enhancements unavailable in the native Windows NT disk class driver. It works with StorageWorks RAID Array controllers to enhance on-line storage availability and fault-tolerance. HszDisk works in single-host and cluster environments to maintain optimum subsystem performance during controller and storageset recovery operations. In Windows 2000, the features provided by HszDisk have been integrated in RaiDisk, obviating the need for this driver.

- **RaiDisk.sys** is a Windows filter driver that provides the primary failover capability in the Secure Path product. RaiDisk supports StorageWorks RAID array multiple-bus mode, multiple path access, and provides all functions required for monitoring I/O and detecting path failures.

- Secure Path Manager (SPM) is a web-based management utility capable of cross-platform Secure Path configurations. This utility displays a graphical representation (GUI) of multiple path configurations, indicating status of a user defined set of hosts, storage systems and paths.

  SPM coexists with other Compaq utilities such as Compaq Insight Manager, StorageWorks Command Console and Enterprise Volume Manager (EVM). SPM enables you to efficiently manage your storage systems in the following ways:

  — Displaying all current path states.

  — Providing remote notification of critical events via paging or email.

- **Secure Path Agent** is a Windows service that communicates with the RaiDisk filter driver on the host server, and Secure Path Manager on the client side, using the TCP/IP protocol and WinSock API. The agent installs on the host server along with the RaiDisk driver.

  To minimize network traffic, display information is relayed from the Secure Path Agent to the Secure Path Manager only when the RaiDisk driver detects changes in the configuration. The Secure Path Agent also notifies StorageWorks Command Console (SWCC) clients when RaiDisk performs path failover or auto-failback operations.

- **Secure Path Setup** supports driver and application installation and de-installation with Windows NT 4.0 and Windows 2000.

Configuration Limitations

Secure Path Manager uses the concept of "profile" to express a working configuration limit. Large configurations can be managed through a single instance of the Secure Path Manager. However, there are certain practical limitations on the configuration size that can be displayed and managed in a single graphical window. The Secure Path Manager profile limits are

- A maximum of 128 servers (host systems)
- Connected to and sharing up to 128 storage systems
- Configured for multiple-bus failover mode.

Secure Path does not provide any mechanism for synchronizing access to, or guaranteeing the data integrity of storagesets shared across multiple standalone hosts or clusters. Access to storagesets is restricted to a single standalone server or a single "clustered" host set.

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

Controller Ownership

Storage systems that are multiple-bus capable generally contain a pair of redundant controllers and support one of the following basic operational models:

- **Active/passive**–In the active/passive model, all storagesets are assigned ownership to one controller of the pair for I/O processing. The other controller is inactive, but available as a substitute in case of failure on the original.

NOTE: MSA1000 **is the only controller that uses the active/passive mo**del.

- **Active/active**–In the active/active model, I/O processing may be routed through both controllers simultaneously, providing better performance in addition to high availability. The RAID Arrays supported by Secure Path implement a modified version of the active/active model. While I/O can be processed simultaneously by both controllers, any given storageset is "owned" or online to a host through only one controller. Ownership of a storageset may be transferred to the other controller at any time through a host-initiated command sequence.

Path Verification

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

Path Verification is useful for detecting failures that affect overall path redundancy before they affect failover capability.

- If a "Preferred" path fails path verification, failover occurs.

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

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

Path Management Behavior Summary

Table 1–1 provides a summary of path management behavior conditioned by the optional features of Secure Path.

Table 1–1: Path Management Behavior Summary

Feature	Behavior/Action
Startup	1. The path to the controller on which the LUN is online is marked **preferred active**. The path to the other controller is marked **alternate available**. 2. If **no online path is** found, an available path online is marked as **preferred active** – and the other path is marked **alternate available**.
Active Path Failure	• Path marked preferred (or alternate) failed and fails to alternate available path. Alternate available path used is marked **alternate active**. • Behavior is the same with I/O or background path verification. • If **LUN is reserved, mark path failed, but** do **not fail to other path on nonowning no**de.

2

Hardware Setup

This chapter provides the following Secure Path hardware setup information:

- Fibre Channel Configuration Installation Prerequisites

- Installing a New RA8000/ESA12000 Secure Path Configuration

- Adding Secure Path to an Existing RA8000/ESA12000 Configuration

Fibre Channel Configuration Installation Prerequisites

Before installing Secure Path on a new or existing Fibre Channel (FC) configuration, first review the RA8000/ESA12000 High Availability Application Notes found on the Compaq web site. They will familiarize you with various high-availability connection layouts for FC devices and cabling.

The application notes present a topological layout of several high-availability options. They also list part numbers, related reference documentation, and discuss restrictions that apply when Secure Path co-exists with MSCS software and FC hardware devices.

The High-Availability Application Notes for FC installations are:

RA8000/**ESA12000 FC**-AL **High Av**ailability **Configurations for W**indows NT – **Intel**	AA-R**H0SE-TE**
RA8000, MA6000/MA8000, ESA12000, and EMA12000 **FC**-**Switch High Av**ailability **Configurations for W**indows NT – **Intel**	AA-R**HH6D-TE**

NOTE: For the most current Application Notes, visit the Compaq website at: www.compaq.com/products/storageworks.

Components Required for RA8000, MA6000/MA8000, ESA12000, and EMA12000 Fibre Channel Installation

Verify receipt of the Secure Path software kit and the FC hardware ordered for the installation. If you are missing any component, please contact the account representative or call the Compaq Customer Services Hotline at (800) 354-9000. The basic requirements for Secure Path operation are listed in Table 2–1

Table 2–1: Secure Path (FC Installation) Prerequisites

Host Feature	Requirement
Platform	**Intel**
Operating System	Windows NT Enterprise Edition, Version 4.0 Windows 2000 Advanced Server Edition
Secure Path Software Kit	SANworks Secure Path v3.1 Enterprise Edition for Microsoft Windows (QB-669AD-SA)
RAID **Storage System(s)**	StorageWorks dual-redundant RA8000/ ESA12000 (FC)
Solution Software Kit	StorageWorks Solution Software V8.6 for Windows NT (QB-65RAE-SA)
StorageWorks Command Console	Storage management software
Host Bus Adapter(s) (and adapter driver)	Supported model for Windows NT - Intel: StorageWorks KGPSA
FC Interconnect Hardware	FC hubs, switches, and connection hardware as required (Application Notes provide detailed equipment part numbers)
Service Tools	Appropriate tools to service the equipment
Technical Documentation	The reference guides for the RAID system, the host server and the Microsoft Windows software

Installing a New RA8000/ESA12000 Secure Path Configuration

This section provides procedures to install and configure a Secure Path topology for *new* FC RA8000/ESA12000 Secure Path configuration. It contains the following major steps:

- Install and check status of hardware
- Configure the RAID system for Secure Path operation
- Install server software
- Shutdown/restart and hardware applications
- Check for successful restart

Install and Check Status of Hardware

1. Install all of the new RAID storage system and FC interconnect hardware (hubs/switches) and cabling according to the instructions provided with the installation documentation shipped with the FC equipment.

2. Establish a serial link to the RAID system using a serial line connection from the host server or from any PC workstation.

3. Obtain RAID controller status using the StorageWorks Command Console (SWCC) Command Line Interface (CLI) or a terminal emulation program, such as HyperTerminal.

Configure the RAID System for Secure Path Operation

4. Using the CLI, complete one of the following substeps to configure the RAID system for Secure Path operation.

   a. For FC-AL configurations, set the Arbitrated Loop Physical Address (ALPA) for HSG80 controllers in the RAID system using the following commands:

   HSG80> **set this_controller port_1_topology=offline**

   HSG80> **set other_controller port_1_topology=offline**

   HSG80> **set this_controller port_1_al_pa=***n+1*

   HSG80> **set other_controller port_1_al_pa=***n+1*

Where n+1 is an available ALPA address selected from the table in Appendix C.

HSG80> **set this_controller port_**1**_topolog**y**=loop_hard**

HSG80> **set other_controller port_**1**_topolog**y**=loop_hard**

HSG80> **set this_controller port_2_topolog**y**=offline**

HSG80>**set other_controller port_2_topolog**y**=offline**

HSG80> **set this_controller port_2_al_pa**=*n*

HSG80> **set other_**c**ontroller port_2_al_pa**=*n*

Where n is an available ALPA address selected from the table in Appendix C.

HSG80> set this_controller port_2_topology=loop_hard

HSG80>**set other_controller port_2_topolog**y**=loop_hard**

b. For FC Switched Fabric configurations, enter the following commands:

HSG80> **set this_controller port_**1**_topolog**y**=fabri**c

HSG80> **set other_controller port_**1**_topolog**y**=fabric**

HSG80> **set this_controller port_2_topolog**y**=fabri**c

HSG80>**set other_controller port_2_topolog**y**=fabri**c

5. Configure the RAID system controllers for multiple-bus failover mode by entering the following commands.

HSG80 > **set nofailo**v**er**

IMPORTANT: The "other" controller will shutdown and must be manually restarted by momentarily depressing the reset button on the controller's front panel. Wait for two minutes for the controller to boot before proceeding.

HSG80 > **set m**ultibus **c**opy=**this**

The controllers will restart in multiple-bus mode.

6. After the other controller has restarted, verify that both controllers are configured for multiple-bus mode by issuing the following command:

HSG80 > **show this**

7. Verify that the data returned to this command includes the statement that the controller is in a multiple-bus dual redundant configuration.