Compaq SANworks

Release Notes - Secure Path Version 2.1D for Sun Solaris

Part Number: AA-RKYEE-TE

Fifth Edition (September 2001)

Product Version: 2.1D

This document summarizes features and characteristics of the SANworks Secure Path Product, Version 2.1D for Sun Solaris systems using StorageWorks Array Controllers for Fibre Channel and SCSI. The Fibre Channel controllers, HSG80 and HSG60 may be configured for Arbitrated Loop (FC-AL) or Fabric (FC-SW). The HSZ80 SCSI controller supports Ultra Wide Differential SCSI. This document provides information not covered elsewhere in the product documentation.

For the latest version of these Release Notes and other Secure Path product documentation, visit the Compaq Storage website at:

http://www.compaq.com/products/storageworks

COMPAQ

Compaq shall not be liable for technical or editorial errors or omissions contained herein. The information in this document 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. 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.

Secure Path Version 2.1D for Sun Solaris
Fifth Edition (September 2001)
Part Number: AA-RKYEE-TE

Table Of Contents

These release notes cover the following major topics:

Intended Audience

This document is intended for customers who are responsible for installing, configuring and maintaining *Compaq SANworks* Secure Path Version 2.1D in their Sun Solaris server environment with any one of the following StorageWorks RAID Arrays:

- RA8000/ESA12000 (HSG80)
- MA8000/EMA12000(HSG80)
- MA6000 (HSG60)
- RA8000/ESA12000 Ultra SCSI (HSZ80)

Secure Path Kit Contents

The SANworks Secure Path Version 2.1D software kit consists of the following:

- The Secure Path documentation set:
  - **Product Description** – *COMPAQ SANworks Secure Path Version 2.1A for Sun Solaris – A High-Availability Solution for Sun Solaris Platforms*
  - **Installation and Reference Guide** – *COMPAQ SANworks Secure Path Version 2.1a for Sun Solaris*
  - Warranty Card
  - **Release Notes** – *COMPAQ SANworks Secure Path Version 2.1D for Sun Solaris* (This document*)*
- A CD-ROM containing documentation and Secure Path Software V2.1D for Sun Solaris.

NOTE: Since Secure Path Version 2.1D is an update release, the Installation and Reference Guide was not updated. Therefore, the Installation and Reference Guide for Secure Path V2.1A is still applicable, and should be used for V2.1D.

Check our website for the latest drivers, technical tips and documentation for SANworks Secure Path at:

http://www.compaq.com/products/storageworks

Enhancements

Enhancements made with the release of Secure Path 2.1D for Sun Solaris are as follows:

- Support for both SCSI-2 and SCSI-3 CCL
- Configuration Utility (spconfig) improved performance
- Improved functioning with Veritas Cluster Server
- Modification to improve driver interaction with dynamic reconfiguration on the Sun Ultra Enterprise 10000 Server.

Modifications to spmt

The command spmt notify was added to spmt to make it easier to manage email recipients.

To improve security considerations, the following commands were removed:

- spmt cli
- spmt restart
- spmt shutdown

These commands are available through SANworks Command Scripter which addresses any security concerns.

Operating System Support

Table 1 lists the hardware and software supported by SANworks Secure Path Software Version 2.1D.

Table 1: Secure Path Version 2.1D Requirements

Host Feature	Requirement
Platform	SPARC; Ultra SPARC
Architectures	4u
Operating System	Solaris 2.6 (32 bit support) Solaris 2.7 (32 and 64-bit support) Solaris 2.8 (32 and 64-bit support)
Free Disk	500KB, before any log files
Fibre Channel Hardware	
Fibre Channel Adapters	Compaq/JNI FC64-1063 (DS-SWSA4-SC) Compaq/JNI FCI-1063 (SWSA4-PC)
Adapter Fcode	**The Fcode on the Compaq/JNI FC64-1063 should be at Version 13.3.7 or greater for proper operation.** (For more information, see Hardware Prerequisites for Secure Path, Page 8.)
Fibre Channel Hub	Compaq 7-port hub 242795-B21 (DS-SWXHX-07) Compaq 12-port hub 245573-B22 (DS-DHGGB-AB)
SAN Switches	Compaq 8 port 380591-B21 (DS-DSGGA-AA) Compaq 8 port 380591-B22 (DS-DSGGA-AC) Compaq 8 port 158222-B21 (DS-DSGGB-AA) Compaq 8 port 158223-B21 (DS-DSGGB-AB) Compaq 8 port 176219-B21 (DS-DSGGC-AA) Compaq 16 port 380578-B21 (DS-DSGGA-AB) Compaq 16 port 380578-B22 (DS-DSGGA-AD) Compaq 16 port 158224-B21 (DS-DSGGB-BA) Compaq 16 port 158225-B21 (DS-DSGGB-BB) Compaq 16 port 212776-B21 (DS-DSGGC-AB)

Table 1: Secure Path Version 2.1D Requirements

Host Feature	Requirement
Controllers	Dual HSG80 Controllers operating one of the following ACS Versions: 8.5F, 8.5G, 8.5P, 8.5S, 8.6F, 8.6G, 8.6P, 8.6S Dual HSG60 Controllers operating ACS Versions 8.5L or 8.6L
Ultra SCSI Differential Hardware	
Ultra SCSI Adapters	Sun X1065A Ultra SCSI Differential (Sbus) Sun X6541A Ultra SCSI Differential (PCI)
Hubs	3 port SCSI hub 401926-001 (DS-DWZZH-03) 5 port SCSI hub 401927-001 (DS-DWZZH-05)
Controllers	Dual HSZ80 Controllers operating ACS Firmware Version 8.3Z

The SAN Switches require the supported minimum firmware version:

- DS-DSGGA-XX- V1.6d
- DS-DSGGB-XX- V2.1.9g
- DS-DSGGC-XX- V2.1.9g

Installation Prerequisites

Hardware Prerequisites for Secure Path

Fibre Channel

Two paths must exist between each server and storage system. Each path must consist of a separate:

- Host Bus Adapter

  On systems that support multiple I/O boards, Compaq recommends that each host bus adapter be installed on separate I/O boards to eliminate the I/O board as a single point of failure.

IMPORTANT: Testing has shown that for each CPQ/JNI fibre channel HBA, a minimum of 32MB of memory is required. CPQ/JNI FCODE of 13.3.7 or later is required for systems that will deploy more than two CPQ/JNI HBAs per I/O board.

The current FCODE version of the JNI adapter is displayed upon system boot as the JNI driver accesses the adapter. An alternate method is to use the OBP and cd in the adapter path itself. (See Solaris OBP documentation for details.)

For FCODE upgrades to the existing JNI adapters go to http://www.compaq.com and visit the driver page. Select the adapter by part number and follow the directions for the FCODE upgrade.

- Fibre Channel Hub or Fibre Channel (SAN) Switch
- HSG80 Controller

  The RAID storage system must be configured for Fibre Channel Arbitrated Loop (FC-AL) or Fibre Channel Fabric (FC-SW) in Multiple-bus Failover Mode.

- Supports a **maximum of 4 RAID systems** per adapter pair.

Ultra SCSI

Two paths must exist between each server and storage system. Each path must consist of a separate:

- Host Bus Adapter

  On systems that support multiple I/O boards, Compaq recommends that each host bus adapter be installed on separate I/O boards to eliminate the I/O board as a single point of failure.

- Ultra SCSI Hub(s) Optional
- HSZ80 Controller

The RAID storage system must be configured in Multiple-bus Failover Mode.

- Supports a **maximum of 2 RAID systems** per adapter pair.

Software Prerequisite for Secure Path

StorageWorks Solutions Software for Sun Solaris version 8.6 must be installed and configured for

a. Fibre Channel support, Loop or Fabric for each adapter in the adapter pair that will be used in the Secure Path installation.

b. Ultra SCSI support for each adapter in the adapter pair that will be used in the Secure Path installation.

NOTE: For installations that have mixed configurations of HSG60, HSG80 and the HSZ80 Raid Arrays, all adapter pairs must be configured prior to the installation of Secure Path.

- At least one LUN on the RAID storage system must be visible on two paths (one path from each adapter) prior to the installation of Secure Path V2.1D.

IMPORTANT: The key to the installation of Secure Path is the configuration of the two paths with the Solutions Software kit. If that installation milestone is met, the installation of Secure Path will be successful.

- Each LUN on the RAID array must be labeled under *format* prior to installing Secure Path to be correctly identified. Invoke format and select each entry on the RAID array. Use the 'TYPE' command and select 0, Auto configure. The device should report itself under the correct controller type and firmware revision. Once that identification is correct, select the 'LABEL' option and write the label to the device. Repeat these steps for each device on the RAID subsystem.

IMPORTANT: It is strongly recommended to configure all storagesets on the RAID subsystem prior to installing Secure Path. Additional target/LUNs may be added later but a server reboot will be required.

Installation Issues

This release of Secure Path Version 2.1D for Sun Solaris can be installed as a new installation or as an upgrade. These options are described below:

New Installation

New installations of Secure Path V2.1D may be of two types:

1. A server that has never been configured with a storage system. For this installation, verify that the steps outlined in Chapter 3 of the *SANworks Secure Path V2.1a for Sun Solaris Installation and Reference Guide* for the hardware installation have been completed and the units on the RAID array are visible from the two adapter paths to the RAID controller.

   This installation is more complex because the installer will have to become familiar with the Solutions Software kit and do an initial installation of that software prior to installing Secure Path. The installer must use the */opt/steam/bin/config.sh* utility that is part of the Solution Software Kit to correctly configure each adapter. Please refer to the Sun Solaris Solutions Software kit Installation Guide.

IMPORTANT: The key to the installation of Secure Path is the configuration of the two paths with the Solutions Software kit. Only if that installation milestone is met will the installation of Secure Path be successful.

2. A server already has a Raid subsystem with a single path installation under the Solutions Software kit. The steps for this installation are similar to those of a new installation with the difference that the installer must pay attention to four key areas:

   a. Conversion from Transparent Failover mode to Multiple-Bus Failover mode at the RAID system. The steps to perform this transition are documented in Appendix E of the *Secure Path V2.1a for Sun Solaris Installation and Reference Guide.* Pay particular attention to any UNIT OFFSET values and connection ACCESS IDs that may already be in place. Also note that controllers configured in multiple-bus failover present four World Wide Port Names (WWPNs). The installation of Secure Path will attempt to honor those offsets.

   b. Addition of a second adapter and configuring that adapter for the RAID array. The addition of the adapter is straight forward and is documented with the adapter. Once the adapter is added to the server, the server must be rebooted.

Configuring the second adapter is important, as it will create a second path to the unit(s) on the RAID array. The installer will have to use the */opt/steam/bin/config.sh* utility to configure the second adapter for the RAID array. Once configured, the server must be rebooted.

With two adapters properly configured, the installer should see the old paths and the new paths.

c. The installer must verify that the server has LUNs for each unit on the RAID array, with one binding for each adapter. Keep in mind that the default bindings in /kernel/drv/sd.conf may not be sufficient to map all the units at the RAID array.

d. The last but most important consideration for the installer is to manually remap the mount points from old device paths (cXtYdZ before Secure Path) to those created under Secure Path.

When Secure Path is installed, it will create a new device path, c5tYdZ, continuing from our example, and the previous bindings of /kernel/drv/sd.conf will be removed in the process.

For example: The old device paths are c3tYdZ for the current RAID device mappings. The system will create c4tYdZ mappings for the second adapter.

Mount points that previously referenced c3tYdZ must now reference the latest c5tYdZ under Secure Path control. Two steps must be performed:

1.Modify the application software to reference the new cXtYdZ values.

2.Edit the following files, as required, to reference the new cXtYdZ values:

– `/etc/vfsmnt`

– `/etc/vfstab`

– `/etc/dfstab`

Automatic vs. Manual entry of WWPNs

World Wide Port names are used in fabric mode with Fibre Channel supported RAID arrays. Previously, the Solutions Software kit would require that the user manually enter the WWPNs of the controller ports to which they want access.

With the latest Solutions Software kit, Version 8.6, in Automatic mode, the driver now probes the fabric and will return the WWPNs to which it has visibility. Unfortunately, in a fabric configuration with Secure Path, the WWPNs must be specific and must map to each path correctly. Since the Solutions Software kit is not designed specifically for Secure Path, the installer must make the adjustments to the WWPNs for each adapter.

This is accomplished by invoking

```
# /opt/steam/bin/config.sh
```

and selecting Option 20, *Add/Modify Adapters* and then selecting Option 4, *Modify an Adapter.*

By selecting the correct number of targets depending on the configuration of RAID boxes, and then assigning the correct WWPNs to those targets, a correct mapping may be created. Unless the correct mappings are created, the target/LUNs will **NOT** be visible from the server and Secure Path will not be able to configure the multiple path storage configuration.

Secure Path Handling of More than Two (2) Paths

At installation and configuration, Secure Path Software will not configure more than two paths to a target/lun. It is possible, however, that additional changes made to the configuration files manually may create a case of more than two paths. Should that happen, Secure Path detects that error at boot time and will preserve only two paths and discard the others.

IMPORTANT: You MUST verify that these two paths are on different controllers in a dual-controller configuration. Refer to Chapter 3 of the *COMPAQ SANworks Secure Path Version 2.1a for Sun Solaris Reference Guide* for more information about valid configurations.

Post-Installation -- Configuration of Secure Path Devices (spconfig)

Previous versions of Secure Path invoked the configuration utility (*spconfig)* automatically during the installation script to create and modify the Secure Path driver configuration files.

With the increased complexity of configurations (number of supported adapters and number of supported RAID arrays) it has been determined that more operator interaction is required in identifying the intended adapters and RAID systems. To that end, invoking the configurator tool, *spconfig*, is now a post-installation step and is documented in Chapter 5 of the *Compaq SANworks Secure Path Version 2.1a for Sun Solaris Installation and Reference Guide*.

IMPORTANT: The key post-installation step for Secure Path is the configuration of the Secure Path software for the server and RAID subsystems. The configuration is implemented with the *spconfig* utility as previously noted.

During the configuration of the Secure Path software *spconfig* assumes that no other software is accessing the controller data during the configuration process. Therefore, it is important that the installer verify that for all RAID array controllers to be configured under Secure Path:

- No CLI serial line connections are in use.
- No SWCC clients are accessing the controllers.
- SWCC Agents are stopped.
- The array controller is not servicing I/O requests from other hosts.
- No SANWorks Management Appliance HSG element manager sessions are active.

The command to invoke is:

```
# /opt/CPQswsp/spconfig -o -p /kernel/drv
```

where *-o* invokes the operator dialogue to select the proper set of adapters and RAID arrays and *-p* is used to identify the path to the configuration files.

Upgrading an Existing Installation

If you already have an earlier version of Secure Path 2.x installed on your server, you may be able to perform an upgrade installation.

This upgrade will only replace the Secure Path executables and will not change your existing configuration. Refer to the following tables to determine if your configuration can support an upgrade.

Table 2: Sun Solaris Version 2.6

Secure Path		**32-bit**	
From	To	Loop	Switch
V2.0	V2.1D	Y	N[1]
V2.1	V2.1D	Y	Y
v2.1a	V2.1D	Y	Y

Table Key
Y = Valid update
N = Invalid update, based on Fibre mode and Solaris OS

[1] Changing your FC topology requires a full Secure Path 2.1D installation. You must use the full kit, not the web update kit.

Table 3: Sun Solaris Version 2.7

Secure Path		32-bit		64-bit	
From	To	Loop	Switch	Loop	Switch
V2.1	V2.1D	Y	Y	Y[2]	Y[2]
V2.1a	V2.1D	Y	Y	Y	Y

Table Key
Y = Valid update
N = Invalid update, based on Fibre mode and Solaris OS

[2] 64-bit kernel mode was not supported with Secure Path V2.1. To run in 64-bit kernel mode, perform the update while in 32-bit mode. After the update is complete, you can reboot with the 64-bit kernel.

Table 4: Sun Solaris Version 2.8

Secure Path		32-bit		64-bit	
From	To	Loop	Switch	Loop	Switch
V2.1a	V2.1D	Y	Y	Y	Y

Table Key
Y = Valid update
N = Invalid update, based on Fibre mode and Solaris OS Version

Secure Path V2.1D Update Procedure

NOTE: The current configuration with the existing Secure Path is NOT changed during this update procedure.

It is strongly recommended that prior to this update the following be verified:

- All I/O has completed to the storage units and further I/O stopped.
- A full backup of the storage has been completed.
- The person performing the update has root privileges.

To install Secure Path 2.1D for Sun Solaris, perform the following steps;

1. Mount the CD-ROM media.
2. Change directory to the Sun Solaris directory. Enter:

   ```
   # cd /cdrom/sp_v21d_sun/solaris
   ```

3. Invoke the update with the following command:

   ```
   # pkgadd -a update -d pkgs
   ```

The update will move the revised executables and scripts to the respective directory areas. For Solaris OS versions that support both the 32-bit and 64-bit kernel, two directory areas will be created under /opt/CPQswsp/bin. They are ld32, for 32-bit support and ld64, for 64-bit support.

For Secure Path version 2.0 and V2.1, one change is made to the /kernel/drv/sd.conf file. The update will place specific binding entries for the Secure Path devices at the head of the file.

4. When the update installation is completed, you must reboot the system.

Converting Fibre Channel Modes

WARNING: Converting from one fibre channel mode to another means performing a new, complete installation for which there are no shortcuts.

For sites that are using Veritas Volume Manager, it will be necessary to export and import the volumes. (Exporting and Importing volumes are described later in these release notes).

For sites that have explicit bindings in /etc/vfstab, the new mapping of devices, cXtYdZ may not be identical to the previous ones. Adjustments may be required.

Secure Path V2.1 supports both fibre channel modes, loop and fabric. For sites that wish to convert from one fibre channel mode to the other, a series of steps is required. Reference documentation is enclosed in parenthesis.

Perform the following steps to convert to Fibre Channel mode:

1. Remove the existing Secure Path software. This step will remove all Secure Path configuration files and the existing configuration will be lost. (Solaris application utility: pkgrm CPQswsp)
2. Reconfigure the Fibre Channel driver to the new mode. (See the Solutions Software kit documentation - specifically config.sh)
3. Reconfigure the RAID storage controllers to the new mode. (See HSG80 CLI and Solutions Software kit documentation)
4. Verify the target/lun mappings with config.sh. (See the Solutions Software kit documentation.)
5. Reboot the server and verify that the target/luns of the RAID array are visible on the two paths. Correct cabling, modes, etc that may have prevented a unit from being accessed from each path. (This is a prerequisite for the installation of Secure Path.)
6. Install Secure Path. Compaq recommends that the latest version, V2.1D be installed. After the spconfig configuration utility executes, reboot the server and verify that the target/luns are now Secure Path devices.

Operating Constraints

Limit on Number of Secure Path Devices

A maximum number of 128 Secure Path devices are supported per Solaris server.

Restriction on Using Secure Path Device as a Boot Device

Secure Path devices cannot be used as boot devices.

Solaris 2.7 and 2.8 Support

Secure Path on Solaris 7 and Solaris 8 is supported in 32-bit and 64-bit mode.

Limit on Number of Paths per LUN

Only 2 paths per LUN on a RAID storage system are supported.

Adapter Pairs of the same Bus Type Supported

Secure Path V2.1D only supports pairs of adapters that are of the same bus type. Adapter pairs must be either Sbus or PCI. Mixed host bus adapter configurations are not supported.

For multiple pairs of adapters on the same server, pairs of Sbus and pairs of PCI adapters are supported. Another way of stating this restriction: The same type of driver must be used for a Secure Path pair of adapters.

NOTE: The Compaq 32-bit Sbus Fibre Channel adapter (p/n DS-SWSA4-SB) is **not** supported in a Secure Path configuration.

Dynamic Reconfiguration Support

Solaris Dynamic Reconfiguration (DR) **is supported** for Solaris V2.7 and Solaris V2.8 with Secure Path V2.1D.

Veritas Considerations

Table 5: Veritas Considerations

Solaris Version	First Watch	Volume Manager	Cluster Server
2.6	V2.5.5.1	**Versions prior to V3.0 may be used with DMP disabled**	V1.1.2
2.7	None	V3.0	V1.1.2
2.8	None	V3.0.4 or later	V1.3

Veritas Volume Manager

Veritas Volume Manager versions prior to V3.0 may coexist with Secure Path V2.1D **only if DMP has been disabled and the procedures defined here are performed.**

IMPORTANT: Veritas Volume Manager 2.5.1 and 2.6.1 are supported if DMP is disabled.

The steps to disable DMP for VxVM are as follows:

1. At the # prompt, enter:

```
# mv /kernel/drv/vxdmp /kernel/drv/DNRvxdmp
# mv /kernel/drv/vxdmp.conf /kernel/drv/DNRvxdmp.conf
# cd /dev/vx ; rm -rf dmp rdmp
# ln -s /dev/dsk dmp
# ln -s /dev/rdsk rdmp
```

2. Edit the file /etc/system and comment out the following entry:

```
forceload drv/vxdmp
```

3. Perform a reconfiguration boot, as follows:

```
# touch /reconfigure
# reboot
```

Installing SANworks Secure Path V2.1D when Veritas Volume Manager is Currently Installed

IMPORTANT: Failure to follow these instructions properly can render your system unbootable. Please carefully read through these instructions before proceeding.

This release note assumes that the Solutions Software kit is already installed and the HSx (HSG60, HSG80, HSZ80) targets are under Veritas Volume Manager control. It is also assumed that the system is set up with a single Fibre Channel host bus adapter to RAID storage system configuration. To install Secure Path when Veritas Volume Manager is already installed, proceed as follows:

1. Start the Veritas Volume Manager Disk Administrator by entering:

   ```
   # vxdiskadm
   ```

2. Select Option 9, “Remove access to (deport) a disk group”.
3. At the following prompt that appears, list all disk groups. Enter:

   ```
   Enter name of disk group [<group>,list,q,?] (default: list) list
   ```

4. At the next prompt, specify all disk groups that contain HSx units that are to be deported.

   Units to be deported may not exist in group *rootdg*. If unsure whether a unit is an HSx unit or not, use the format command and look at the device description.

IMPORTANT: When prompted if you want to “Disable (offline) the indicated disks?”, select “**yes**”.

5. Power down the system, install the new adapter, and bring the system back up, as described in Chapter 3 of the *Compaq* SANworks *Secure Path Version 2.1a for Sun Solaris Installation and Reference Guide*.
6. Upon system reboot, start the Veritas Volume Manager Disk Administrator, using the command:

   ```
   # vxdiskadm
   ```

7. Select option 11, “Disable (offline) a disk device”.
8. At the following prompt that appears, list all disk devices. Enter:

   ```
   Select a disk device to disable [<address>,list,q,?] list
   ```

9. At the next prompt that queries disk devices to disable (offline), specify all disk devices that contain HSG units that are to be disabled.

In the example below, d0, d1 and d2 have been disabled (offlined).

```
DEVICE      DISK        GROUP       STATUS
c0t0d0      rootdisk    rootdg      online
c1t65d0                             offline
c1t65d1                             offline
c1t65d2                             offline
c2t65d0                             offline
c2t65d1                             offline
c2t65d2                             offline
```

10. Quit from the Veritas Volume Manager Disk Administrator
11. Install the Secure Path package according to the standard installation procedures defined in Chapter 4 of the *Compaq SANworks Secure Path Version 2.1a for Sun Solaris Installation and Reference Guide*.
12. Reboot the system with a configuration boot (per installation instructions).
13. Start the Veritas Volume Manager Disk Administrator using the command:

    ```
    # vxdiskadm
    ```

14. Select option 8, “Enable access to (import) a disk group”.
15. At the following prompt that appears, list all disk groups. Enter:

    ```
    Enter name of disk group [<group>,list,q,?] (default: list) list
    ```

16. At the next prompt, import all disk groups that were previously deported.
17. Quit from the Veritas Volume Manager Disk Administrator.
18. Ensure that the correct disks are under Veritas Volume Manager control by entering:

    ```
    # vxdisk list
    ```

The coexistence of Secure Path with Volume Manager is now established.

NOTE: If Secure Path for Sun Solaris is removed, this process must again be followed to ensure access to Veritas Volume Manager controlled volumes and proper operation of the Sun Solaris server.

Possible Error Messages

There is a required order between the startup of Secure Path and the Volume Manager configuration daemon.

Volume Manager will start up without errors as long as one disk configured in *rootdg* is not a Secure Path device.

However, if Volume Manager is configured with Secure Path devices only, messages similar to the following will be displayed on the console during boot:

```
VxVM starting in boot mode...
vxvm:vxconfigd: ERROR: enable failed: Error in disk group configuration copies
No valid disk found containing disk group; transactions are disabled.
vxvm:vxconfigd: FATAL ERROR: Rootdg cannot be imported during boot
.
.
.
VxVM general startup...
vxvm:vxconfigd: ERROR: enable failed: Error in disk group configuration copies
No valid disk found containing disk group; transactions are disabled.
vxvm: Vold is not enabled for transactions
No volumes started
vxvm:vxrecover: ERROR: IPC failure: Configuration daemon is not accessible
```

Once the server has finished booting, enable Secure Path devices by issuing the following commands:

```
# vxdctl enable
# vxdg import disk_group
# xvvol –g disk_group startall
```

Repeat the last two commands for each disk group.

SWCC Agent Failover for Veritas Cluster Server

For installations using Veritas Cluster Server in conjunction with the StorageWorks Command Console for maintenance and monitoring of the RAID subsystem, two scripts have been provided on the installation CD in

```
/cdrom/cdrom0/sp_v2.1d_sun/Veritas
```

to implement the automatic failover of the SWCC agent.

The first script, **install_SWCC_failover.sh** will install the files necessary for Veritas Cluster Server to control the SWCC Agent failover. The script creates the `opt/VRTSvcs/bin/SWCC` directory and copies the following files to it:

/opt/VRTSvcs/bin/SWCC/online

/opt/VRTSvcs/bin/SWCC/offline

/opt/VRTSvcs/bin/SWCC/monitor

After the files are copied to the directory, the cluster configuration file is set to Read-Write and the SWCC type is added. The cluster administrator creates a **resource name** and identifies a **service group** to which to add the resource. The cluster configuration file is set to Read-Only. The cluster administrator must add the dependencies as required for the newly created resource.

The second script, **remove_SWCC_failover.sh** will delete the installed VRTS types, resource and files. It deletes the SWCC type, the user named resource and the /opt/VRTSvcs/bin/SWCC directory and the following files:

/opt/VRTSvcs/bin/SWCC/online

/opt/VRTSvcs/bin/SWCC/offline

/opt/VRTSvcs/bin/SWCC/monitor

Notes about Installations

- The SWCC agent must be installed and configured on all systems in the Cluster. Verify that each server has the Access Device identified and that the RAID system(s) are seen by each server.
- The SWCC agent may only be running on one server in the cluster.
- Install the SWCC Agent failover script on one and only one node of the cluster.
- Configure the SWCC Agent on one and only one resource group in the cluster.
- No error checking is done on the user input. Verify that the data entered is valid to prevent operational errors later.

spmt Considerations

When using the Secure Path Management Tool, *spmt*, there are two important considerations:

Some of the operations that may be performed with *spmt* will not complete immediately. If */opt/CPQswsp/bin/ld32/ldinfo or /opt/CPQswsp/bin/ld64/ldinfo* is invoked, it is possible that the device state changes have not completed and stale information will be displayed. It is recommended that a grace period of 5 seconds be allowed for changes to fully be effected. This time allotment should be adjusted for systems with heavy I/O and/or a large number of LUNs.

Partitioned Storage Sets

While each partition of a partitioned storage set is identified and defined as other units on the RAID storage system, the design of the HSG80, HSG60 and HSZ80 controllers imposes a restriction that **all partitions must be assigned to the same controller and the same host.**

Under Secure Path, if partitions (units) have a preferred path set at the controller, then all such partitions must have the same preferred path. Failover and failback events of a partitioned unit apply to all partitions of the same storage set.

Known Problems

Boot Message "ddi_model_convert_from multiply defined"

On system boot, the message “ddi_model_convert_from (multiply defined)” is displayed on the console. This message may be disregarded.

fcaw/fca-pci Driver Message

On system boot, fcaw (Sbus driver) and fca-pci (pci driver) for Fibre Channel identifies itself as Version 2.5.9 for Solaris 2.5 and 2.6. In fact, this driver supports Solaris 2.5.1 through 2.8.

HSZ80 Target = 0 and LUN = 0 sd.conf Entry Conflict

The HSZ80 as well as the HSG60 and HSG80 devices will have bindings created through the entries in sd.conf as configured by Secure Path V2.1D However, as a true SCSI device, the HSZ80 devices will have bindings created through the default sd.conf entry of Target =0, LUN = 0. This duplicate binding is unintentional and undesirable as the storage unit should be under the exclusive control of the Secure Path software for I/O, failover, display, and so on.

To avoid the conflict created by the duplicate binding, the system manager/installer has two solutions available.

1. If the original `/kernel/drv/sd.conf` entry of Target = 0 LUN = 0 is unused, it may be removed or commented out.
2. When creating the Target/LUN assignments at the HSZ80 Raid Array, do not create a unit at Target =0, LUN =0.

PCI Dual-ported Ultra-SCSI Adapters with the HSZ80

After Secure Path is installed, manually invoke the configuration utility `/opt/CPQswsp/bin/spconfig` to create and edit the configuration files in `/kernel/drv.`

One of the actions of spconfig is to remove the adapter entries from `/kernel/drv/sd.conf` that are being used in the Secure Path configuration.

An example of the PCI dual-ported entries 1st Channel and 2nd Channel are shown as follows:

```
name="sd" parent="/pci@1f,2000/scsi@1" target=0 lun=0;

name="sd" parent="/pci@1f,2000/scsi@1,1" target=0 lun=0;
```

Using a string comparison, spconfig removes entries that match the specific channel. Unfortunately, this leaves the other channel entries in the configuration file and will prevent correct bindings to the target/luns of the storage system.

NOTE: The extraneous entries for the other channel must be removed.

HSZ80 and Restarting a Controller

Testing has found that there is a problem with the isp driver for the Ultra-SCSI Differential Sbus adapter (X1065) in the way that it handles a reset request to the HSZ80 controllers.

This problem manifests itself when a RAID controller is restarted while a host bus adapter is in an Active State.

The controller at the HSZ80 RAID array will restart correctly, but the adapter will no longer be able to communicate with the devices on the RAID array. Additionally, system panics have occurred when I/O is again issued along that path.

The current workaround is to quiesce the adapter, restart the controller and then reconfigure the adapter. If these steps are not followed, the only recourse is to reboot the server.

For example:Assume the adapter is pci100,f2/pci@1f and *spmt* will display the instance as fca-pci0 and assume and the controller serial number is ZG825000433

```
# spmt remove -a  fca-pci0
```

Restart the controller

```
# spmt reconfigure -a fca-pci0
```

NOTE: Compaq has created a Problem Case with Sun support and Sun is currently working towards an update to the isp driver.

Removal of Unused /dev/*dsk Entries

A prerequisite for the installation of Secure Path is that at least one LUN is visible from two paths (one path per adapter) through the Solutions Software for SUN Solaris. When the server defines the paths, device files in /dev/dsk and /dev/rdsk are created pointing to the specific c*X*t*Y*d*Z*.

When a Secure Path new installation is completed, and the reconfigure boot is performed, the /dev/dsk and /dev/rdsk files are handled differently by Solaris per operating system version.

Under Solaris V2.6, the /dev/*dsk file cleanup is performed automatically.

Under Solaris V2.7 and V2.8 the /dev/*dsk file cleanup is **not** performed automatically. Solaris has implemented a new utility/command, *devfsadm* (1M) that may be invoked to remove the dangling links that are remaining. We strongly recommend that this command be invoked to remove any unused device links and verify, using *format* that all the target/luns of Secure Path are visible. Cleanup of the dangling logical links is performed with:

```
# devfsadm -C
```

spconfig Limitations

During configuration of the Secure Path software, spconfig assumes that no other software is accessing the RAID Array Controllers. Therefore, it is important that the installer verify the following situations exist for **all** RAID controllers being configured under Secure Path:

- No CLI serial line connections are in use.
- No SWCC Agents or Clients are accessing the controllers.
- The RAID Array Controller is not servicing I/O requests from other controllers.
- SANWorks Management Appliance HSG Element Manager is not accessing the controllers.

CCL Device Automatically Configured by *spconfig*

The Command Console LUN (CCL) is used by the server to communicate with the storage system. For the HSG80 and the HSG60, it is a virtual LUN that can relocate itself as necessary on the RAID system.

The CCL may be in one of two states at the controller: Enabled or Disabled. In Compaq platform kits for Sun Solaris installations, it is recommended to disable the CCL. This is because the CCL is neither readable nor writeable for normal I/O and *format* will be unable to label it. However, it is available for inquiry at a code/program level.

In the Secure Path implementation, if the CCL is enabled, an entry for the CCL is created in three configuration files documented in Chapter 8 of the Installation and Reference Guide. The files: *ldLite.conf*, *mda.conf*, and *sd.conf* in */kernel/drv* will contain entries for each CCL but the entries will be commented out.

If this installation has a user-written application that performs SCSI inquiries directly to the controller under program control, then these entries should be uncommented and the system rebooted with a reconfiguration boot.

NOTE: If this installation has a user-written application that uses the CCL, adding or deleting units on the subsystem may cause the CCL to move to another LUN. Adjustments must be made to the *ldLite.conf*, *mda.conf* and possibly the *sd.conf* file to reflect this change.

NOTE: USE CLI> **SHOW THIS_CONTROLLER** and CLI> **SHOW OTHER_CONTROLLER** to verify the LUN ID of the CCL.

Removing Secure Path Logical Device Links (Solaris 7 and 8 only)

During the installation and configuration of the Secure Path software, a new set of device files are created in the */dev/dsk* and */dev/rdsk* directories.

After a system reboot, the dangling logical links may be removed with the command

```
# devfsadm -C
```

Change of Access Device for SWCC Access

Configurations that use the StorageWorks Command Console (SWCC) for RAID subsystem maintenance and monitoring, will have identified a device path for communication to the RAID system. For example, c3t4d0.

When Secure Path is installed, if the device path becomes a part of the Secure Path configuration, during a reboot or SWCC agent restart, a message will be displayed to the user notifying them that the old device path is now invalid.

To modify the RAID's access path, invoke `/opt/steam/bin/config.sh` and either Remove a Subsystem (Option 14) and Add a Subsystem (Option 13) or modify the existing entry using Option 15. Remember that any changes to the Agent configuration files require the SWCC Agent to be restarted.

Pseudo Devices and Secure Path under Solaris 8

Customers familiar with Secure Path Version 2.1 have seen the Secure Path specific entries in the `/kernel/drv/sd.conf` file. On Solaris 2.6 and 2.7 the Secure Path entries for sd.conf were of the form:

```
name ="sd" parent="/pseudo/ldLite@0" target=16, lun=0;
```

These entries matched the entries in ldLite.conf with designations of targ**N**-devname where **N** started at 0 and were consecutive integers used to account for each target/lun under Secure Path control.

Under Solaris 2.6 and 2.7, the creation of sd bindings for sd devices was handled in such a way that there was a range of values for sd devices and a range of values for pseudo devices and the values never conflicted.

Under Solaris 2.8, the handling of the pseudo devices changed in such a way to create collisions between the sd devices and the pseudo devices. As a result, a workaround was created to resolve the collisions by starting the pseudo devices at a large integer value (200 was chosen). Thus the entries under ldLite start with targ**200**-devname and the corresponding entries in sd.conf start at 200 also.

The separation of sd devices and pseudo devices will not be problematic unless the sd devices on a specific server require more than 200 entries of the form shown below:

name="sd" class="scsi" target=**Y** lun=0 where **Y** is 200 or greater.

In that case, the starting value for the ldLite and sd.conf values for the pseudo devices must be reset to a larger value, for example, 300.

Compaq has created a Problem Case with Sun support and Sun has now escalated the problem to Bugid 436328.

Data Replication Manager (DRM) with Secure Path Version 2.1D

It is recommended that you visit the website at: http://compaq.com/storage for updated DRM software support.

Secure Path and the Sun Ultra Enterprise 10000 System

Secure Path uses the sd class driver for bindings to the target/luns of the storage system that it communicates with.

Compaq has discovered that if there are no SCSI devices on the Ultra Enterprise 10000 (UE10K) system (or domain) either for purposes of booting (disk) or software loading (CD-ROM), the sd class driver does not load and the Secure Path devices will not have bindings created.

Secure Path will install correctly but upon reboot, the bindings and /dev/dsk/cXtYdZ links as well as device nodes under the /devices/pseudo/ldLite@0 path will not be created.

We have verified that this problem is unique only to the UE10K system. Additionally, we have found that the /etc/system forceload /drv/driver_name fails to perform as documented.

While Compaq continues to explore alternate solutions to this problem, the temporary workaround solution is to add at least one SCSI device to the domains used for Secure Path.

Avoiding Problem Situations

Create Only Two Paths to a RAID Storage Unit

CAUTION: Secure Path requires that **only two** paths exist from the server to the LUN on the RAID storage system. Should a configuration be constructed such that more than two paths are available to the Secure Path implementation, the system will post a message that there have been more than two paths found and will use two, discarding the others.

Adding and Deleting LUNs

When LUNs are added or removed on the RAID storage system after Secure Path has been initially configured, the Secure Path configuration files must be edited to reflect the change. Full details are provided in Chapter 5 of the *Compaq SANworks Secure Path Version 2.1a for Sun Solaris Installation and Reference Guide*.