Compaq StorageWorks

Release Notes

StorageWorks RA7000/ESA10000 Secure Path High Availability Solution for Sun

This document summarizes features and characteristics of StorageWorks Secure Path Version 1.0 for Sun Solaris, a High-Availability software solution for Sun Platforms for use with StorageWorks RA7000 and ESA10000 RAID Storage Systems.

These *Release Notes* provide information for StorageWorks Secure Path Version 1.0, High-Availability Solutions Software not available elsewhere in the product documentation, and takes precedent over those sources. Individuals responsible for configuring, installing, and using this software should use this document.

Visit Our Web Site for the Latest Information

Compaq is continually making additions to its StorageWorks solutions product line. Please check the Compaq web site for more information on the complete line of storage products, product certification, technical information, updates, and documentation. This information can be accessed at:

http://www.compaq.com/storageworks

NOTE: Read this entire document before installing or upgrading the software.

These Release Notes include the following sections:

- Operating System Support
- Host Adapter Support
- Hardware and Software Support
- Clarifications
- Operating Constraints
- Known Problems
- Avoiding Problem Situations
- Documentation Additions and Corrections

1 OPERATING SYSTEM SUPPORT

StorageWorks Secure Path Software is supported on the following operating systems:

- Solaris 2.6
- Solaris 2.7

The following Sun patches must be installed on your system for Secure Path to run properly:

Your system may already have these patches installed. Check using
`# showrev -p`

Table 1. Required Sun System Patches

Version	Patch needed
Solaris 2.6	#106226-01 #105600-10 #105181-17 #106125-05
Solaris 2.7	#106541-08 #107544-03

2 HOST ADAPTER SUPPORT

The following host adapters are supported:

- SUN SBus X1065A Ultra FWD SCSI Adapter
- SUN PCI X6541A Ultra FWD SCSI Adapter

3 HARDWARE SUPPORT

The following StorageWorks RAID subsystems, running HSOF software revision level 7.7, are supported:

- RA7000
- ESA10000

4 OPERATING CONSTRAINTS

4.1 Limit on Number of Safe Devices

There is a limit of 512 safe devices that can be supported per server.

4.2 Restriction on Using Safe Device as a Boot Device

Safe devices cannot be used as boot devices.

4.3 Invalid or Missing Registration Key

If the registration key is incorrect or missing, an appropriate error message is not always displayed on Solaris 2.5.1. Check the registration key, if you see the following message on the console and/or in the system message file:

```
INIT: Command is respawning too rapidly. Check for possible
errors
id: ms "/usr/bin/priocntl -e -c /etc/hszdaemon
```

To check the registration key, type the following:

```
# cat /etc/secure_path_registration
```

If the file is missing or the key displayed does not match the key listed in the *Read Me First* document, re-enter the key by either editing the file */etc/secure_path_registration* or type the following:

```
# echo Your Registration Key Here > /etc/secure_path_registration
```

4.4 Formatting Safe Devices

When safe devices are repartitioned and relabeled using **format**, you must execute the following steps afterward:

```
# /etc/hszsafemt toggle dev=<safe_ID>
```

for each repartitioned device

```
# format
```

```
# /etc/hszsafemt restore
```

This causes the "sd" partition map on the failover path to be updated, avoiding I/O error after failover.

4.5 Hszdaemon Startup

After reboot, **hszdaemon** and **hszsafemt display** see no device messages for a while and sometimes a path is missing. The configuration and management utilities are not useable until the **hszdaemon** has completed initialization.

4.6 Using Utilities During Path Failover

During a path failover, **hszsafemt** will appear to hang. Once the failover is complete, the session will resume.

4.7 Changing the Active Path in a Multihost Environment

In a multihost environment, the commands **hszsafemt toggle** and **hszsafemt restore** will affect only the safe devices that are currently active on the local host. In order to change the devices that are active on the other host, the commands must also be executed on the other host.

5 KNOWN PROBLEMS

5.1 Unknown Device when # *format* is invoked

The *format* command will display “unknown device” if the COMMAND CONSOLE LUN on the RAID controller is enabled. If "unknown device" is displayed, exit *format* and establish a *tip* serial line to the RAID controller. Disable the COMMAND CONSOLE LUN by typing:

HSZ70> set this NOCOMMAND_CONSOLE_LUN <enter>

HSZ70> restart other <enter>

HSZ70> restart this <enter>

5.2 Accessing the CLI

There can be problems when accessing the RAID CLI using **hszsafemt cli** and a **tip** CLI session at the same time. The system may hang. Do not run a **tip** CLI session at the same time as **# hszsafemt cli**.

5.3 Safecf Crash

If the file */etc/safe_to_volnum* is corrupt, **safecf** will crash. This file should not be edited.

5.4 Blank Display when all Paths Fail

When both paths are failed, **hszsafemt display** will not print any output for that device.

6 AVOIDING PROBLEM SITUATIONS

6.1 Starting the hszdaemon in a multihost environment

The command **safeinit** offers a "startnr" option, which installs a single-user startup script, */etc/rcS.d/S62safe-startup,* but without **hszsafemt restore** in it. This is useful in a multi-host environment. It prevents devices being moved by one host when the other may have specifically moved them to the other path.

7 DOCUMENTATION ADDITIONS AND CORRECTIONS

7.1 SWCC

If SWCC is going to be used, the StorageWorks Command Console Agent must be configured to use safe devices. To do this, run the configuration script (refer to section 4-12 of the *Getting Started – HSZ70 Solutions Software V7.7 for Solaris 2.x).*

7.1.1 Installing SWCC with Secure Path V1.0 Previously installed;

Select Option 13, Adding a Subsystem. The auto-configure will fail because it is looking for c*N* controller values on the RAID subsystem. It will report that no subsystems have been found. Select the manual configure and specify a valid “safe*N*c” value even though it requests a “c*N*t*N*d*N”* value. Finish SWCC setup according to the instructions in the *HSZ70 Solutions Software V7.7 for Solaris 2.x* guide.

7.1.2 Installing Secure Path after SWCC has been installed and configured

After installing Secure Path, SWCC will no longer be able to see the RAID system. This is due to the fact that Secure Path removes the c*N*t*N*d*N* controller values and replaces them with safe*N* values. This can be corrected by running the config.sh utility and selecting Option 15, Modify a Subsystem and changing the value of the Access Device to a valid "safe*N*c" value. The agent must then be stopped and restarted again through Option 3, Start/Stop an Agent.

7.1.3 Command Console Client

When the RAID subsystem is configured for MULTIBUS_FAILOVER, the controllers are not displayed by the SWCC Client and cannot be accessed.

An updated version of the SWCC Client Software may be available. Please check our web page for periodic updates to the SWCC Client Software.

7.2 Using VERITAS Volume Manager with Secure Path

When using VERITAS Volume Manager with Secure Path the correct installation order is to install Secure Path first and reboot with the new Secure Path 'safe' devices. Then install Volume Manager following the steps as listed below.

1. Use vxinstall and encapsulate the Boot Disk.
2. Reboot the server. This is a dual reboot process initiated by Volume Manager with no user intervention required.
3. Invoke /opt/SWSP/safevxvm setup
4. Invoke /opt/SWSP/safevxvm init
5. vxdg init *safe_dg safe0c safe1c safe2c etc.* where *safe_dg* is a user defined device group and *safe1c, safe2c, etc.* are the safe devices under Secure Path.

The Secure Path devices are now a Volume Manager disk group and can be managed and configured as any other Volume Manager disk group.

7.3 Using FirstWatch with Secure Path

NOTE: FirstWatch is only supported on Solaris 2.6.

To use Secure Path with Veritas FirstWatch version 2.2.5.1, you must install Secure Path and configure FirstWatch as described in this section.

You should have the Veritas FirstWatch Installation and Configuration Guide available for reference.

7.3.1 New Installation

Follow the instructions in this section if this is the first time you are installing FirstWatch with Secure Path devices.

1. Install Secure Path following the instructions described in Chapter 3 of the StorageWorks RA7000/ESA10000 Secure Path High Availability Solution for Sun Installation Guide.
2. Determine which Secure Path safeN devices you will use as file system devices to be shared under FirstWatch. Partition the selected volumes using the Solaris **format** utility.
3. Create file systems on the selected Secure Path devices using the appropriate utilities for the type of file system you will use. For example, if you are using the standard Solaris UFS file system, enter the following command:

   ```
   # newfs /dev/rdsk/safeNp
   ```

   where N is the safe device instance of the selected volume, and p is the partition identifier in the range [a-h] (remember that Secure Path partitions [a-h] correspond to sd slices [0-7]).
4. Create mount points for the new file systems.
5. Install and configure Veritas FirstWatch. Be sure to use the safe devices as the shared data disks. The PRIMARY_MOUNTS and TAKEOVER_MOUNTS variables in the ha.env file need to be set. For example:

   ```
   PRIMARY_MOUNTS=”/dev/rdsk/safeNp /dev/dsk/safeNp /first”
   TAKEOVER_MOUNTS=”/dev/rdsk/safeNp /dev/dsk/safeNp /second”
   ```
6. Reboot the server.

7.3.2 Installing Secure Path on a System that already has FirstWatch in Place

Follow the procedure in this section if you have already installed FirstWatch and need to reconfigure it for Secure Path.

1. Install Secure Path following the instructions described in Chapter 3 of the StorageWorks RA7000/ESA10000 Secure Path High Availability Solution for Sun Installation Guide.

WARNING

Do not reboot your system at this time

2. The shared data disks are specified in the ha.env file as cNtNdNsN devices. These cNtNdNsN devices must be transitioned over to safe devices. Match the /dev/(r)dsk/cNtNdNsN devices with the corresponding /dev/(r)dsk/safeNp devices by using the command **/etc/hszsafemt display**. After editing the ha.env file to include the safe devices, reboot the server.

7.3.3 Remajoring Devices

The major numbers for the safe devices that are shared must match on both servers. Check the major number of the safe device on each server by typing:

```
# ls –lL /dev/rdsk/safeNp
```

The output would appear as:

```
crw-------   1 root   sys   161,   26   Jul 29 14:21 /dev/rdsk/safeNp
```

The major number in this example is 161.

To change the major number of the safe device, first determine what major numbers are available. The */etc/name_to_major* file contains a list of the system device types and their associated major numbers.

WARNING

Different system device types can not have the same major number on a system.

The setSPmaj script assigns new major numbers to the safe devices.

```
# setSPmaj <new major number>
```

After running the setSPmaj script, perform a reconfiguration reboot for the changes to take effect. The recommended method is shown below.

```
# touch reconfigure
# reboot
```