Compaq SANworks

Release Notes -
Secure Path Version 3.0 for Sun Solaris

Part Number: AA-RKYEF-TE

First Edition (November 2001)

Product Version: 3.0

This document summarizes features and characteristics of SANworks Secure Path Version 3.0 for Sun Solaris systems, using StorageWorks Array Controllers for Fibre Channel Switched Fabric. For the latest version of these Release Notes and other Secure Path documentation, visit the Compaq storage website at:

http://www.compaq.com/storage/

COMPAQ

Release Notes - Secure Path Version 3.0 for Sun Solaris
First Edition (November 2001)
Part Number: AA-RKYEF-TE

Release Notes Contents

These release notes cover the following major topics:

Intended Audience

This document is intended for customers who purchased Compaq SANworks Secure Path Version 3.0 for Sun Solaris and are responsible for installing, configuring and maintaining this product in their Sun Solaris server environment with any one of the following StorageWorks RAID Arrays:

- RA8000/ESA12000 (HSG80)
- MA8000/EMA12000 (HSG80)
- EMA16000 (HSG80)
- MA6000 (HSG60)

Secure Path Kit Contents

The Secure Path Version 3.0 for Sun Solaris kit includes:

- Compaq SANworks Secure Path Version 3.0 for Sun Solaris Quick Specification, part number AV-RR6ZA-TE
- *Compaq SANworks Secure Path Version 3.0 for Sun Solaris Installation and Reference Guide*, part number AA-RKYDE-TE
- Warranty Card
- Compaq SANworks Secure Path Version 3.0 for Sun Solaris Release Notes, part number AA-RKYEF-TE (this document)
- Compaq SANworks Secure Path Version 3.0 for Sun Solaris CDROM

Additional documentation, including white papers and best practices documents, are available via the Compaq website at:
http://www.compaq.com.

Features

Secure Path Version 3.0 for Sun Solaris provides the following features:

- Multi-pathing up to 32 paths per LUN
- Multiple path driver that includes
  - — Path verification for all paths
  - — Auto restore for failed paths
  - — Load balancing using a round robin process
- Dynamic uninterrupted operation for
  - — Add/Delete of LUNS
  - — Controller replacement
- Secure Path Management Utility (spmgr)
- Event Notification via email
- Controller Partition Support for clustered and non-clustered HSG80 and HSG60 storage systems with Homogeneous hosts only.

Operating System Support

Table 1 lists the hardware and software supported by SANworks Secure Path Version 3.0 for Sun Solaris.

Table 1: Secure Path Version 3.0 for Sun Solaris Requirements

Host Feature	Requirement
Platform	Sun SPARC
Operating System	Solaris 8, Solaris 7, Solaris 2.6
Kernel Mode	32-bit; 64-bit
Sun Hardware	Sun4u Architecture only
Secure Path Software Kit	SANworks Secure Path V3.0 for Sun Solaris
RAID Storage Systems	StorageWorks RA8000/ESA12000, MA8000/EMA12000 or MA6000 (FC) with either HSG60 or HSG80 dual controllers using ACS V8.5 or V8.6 (See note after this table.)
Solution Software Kit	StorageWorks Solution Software for Sun Solaris, V8.5c or 8.6
Host Bus Adapters	FC PCI 32-bit Adapter 380576-001 (SWSA4-PC) FC Sbus 64-bit Adapter 123503-001 (DS-SWSA4-SC)
Required Patches	Solaris 2.6: 105375-18, 105357-04, 105356-10, 106226-01, 105181-29, 106429-02, 106125-08, 105210-38 Solaris 7: 106541-16, 107544-03, 106980-16 Solaris 8: 108528-09, 109793-07, 111049-02, 110912-01, 111293-03, 110383-01, 110794-02, 108827-10

Table 1: Secure Path Version 3.0 for Sun Solaris Requirements

Host Feature	Requirement
Fibre Channel SAN Switches	Compaq 8 port 380591-B21 (DS-DSGGA-AA) Compaq 8 port 158222-B21 (DS-DSGGB-AA) Compaq 8 port 176219-B21 (DS-DSGGC-AA) Compaq 8 port 158224-B21 (DS-DSGGB-BA) Compaq 16 port 380578-B21 (DS-DSGGA-AB) Compaq 16 port 158223-B21 (DS-DSGGB-AB) Compaq 16 port 212776-B21 (DS-DSGGC-AB) Compaq 16 port 158225-B21 (DS-DSGGB-BB)
GBICs	FC Optical GBIC 380561-B21 (short wave)

NOTE: Running ACS V8.6, the RAID storage system must have:

- Hardware revision E08 or higher HSG80 controller modules
- A minimum of 128 MB of cache. If mirrored cache is enabled, an additional 128 MB of cache per controller is required.

Refer to the *ACS Solution Software for HSG80 Release Notes* for details.

NOTE: SCSI or Fibre Channel Arbitrated Loop configurations are no longer supported.

Configuration Limitations

Table 3 shows the configuration limits for Secure Path for Sun Solaris.

Table 3: Configuration Limitations

Parameter	Minimum	Max Qualified	Max Supported
Host Bus Adapter support	1	8	16 HBAs per Controller Pair
Storage arrays per host	1	8	128

Avoiding Problem Situations

The following sections list problems that may arise during Secure Path operation and how to avoid them.

General Notes

Dynamic LUN addition

The Solaris Operating System does not support dynamically adding new scsi disk devices to a system. The issue lies in the behavior of the scsi disk driver, sd. The *sd* driver only checks it's configuration file *(sd.conf)* when it is loaded, typically when the system is booted. If new entries are added to the *sd.conf* file, the only way to force the driver to read them is to unload and reload the driver. This is impossible when a system has scsi disks, using the *sd* driver, mounted.

We overcome this limitation, and provide truly dynamic LUN addition, by adding extra entries to the *sd.conf* file. These extra entries are added by the spconfig utility when it configures your system files during the installation. By default, 199 extra entries are added.

On servers with multiple storage systems with multiple paths, this can result in a large number of extra entries taking up system resources. If you do not require such a large number of extra LUN entries, you can reduce the number of extra entries by running *spconfig* with the -d option. This option allows you to specify the number of extra LUN entries from 0 to 255. Your system must be rebooted after running *spconfig*, so that the new sd.conf settings are recognized.

Note that only LUNs can be dynamically added to existing targets. Any time you are adding a new storage system World Wide Port Name (WWPN) to your configuration, your server must be rebooted. This includes adding new controllers and/or paths. These steps are documented in step 6 of the upgrade process on page 5-6 of the *Compaq Secure Path Version 3.0 for Sun Solaris Installation and Reference Guide.*

Path Locked message during reboot

During reboot, when *spinit* is executing, you will see the following warning message:

```
WARNING: Path hsx-6-34-6 locked, must be quiesced prior to detach
```

This message can be safely ignored.

Error during reboot with Solaris 2.6

When rebooting your server with Solaris 2.6, you will see following error message:

```
Devlinks: Line 124 in configuration file: Devpat Field 'rcc\N0@\A0' incorrect, Ignoring.
```

This message can be safely ignored.

Starting/Stopping spagent

Do not start or kill *spagent* directly, always use the *spinit* script to start and stop the agent.

The proper syntax to start *spagent* is:

```
/etc/init.d/spinit start
```

The proper syntax to stop *spagent* is:

```
/etc/init.d/spinit stop
```

Fault in private data message during reboot

During a reboot, you will see the following warning:

```
WARNING: devinfo: fault in private data at 30000242e40
```

This message can be safely ignored.

Required patches

Required patches are listed in Table 1 of this document. The Secure Path installation will not verify that the required patches are loaded. The system administrator is responsible for ensuring that all required patches are loaded.

Selective Storage Presentation with Secure Path Version 3.0.

Compaq recommends the use of Selective Storage Presentation (SSP) in a Secure Path environment. SSP is documented in the HSG60 and HSG80 Array Controller CLI Reference Guides. In a Storage Area Network (SAN) environment, it is always good practice to use SSP in order to minimize chances of data corruption by restricting which Host Bus Adapters (HBAs) have access to certain LUNs on the array at the RAID controller level.

There are also instances when the *spconfig* utility can configure HBAs that may not have been intended for use in the Secure Path environment when SSP is not used. This can only happen when less than the total number of HBAs installed in a host are to be used in the Secure Path configuration. Specifically, if a physical path exists between an HBA and a port on the array that is being used by Secure Path, the LUNs on the array have access set to “all” and the HBA not intended for Secure Path has the HBA driver (CPQfcaw or CPQfcaPCI) loaded, the HBA can be configured into the Secure Path environment. This will be avoided with the use of SSP on the storage array.

Command Console LUN

Do not add a Command Console LUN (CCL) to Secure Path configuration. This may appear to work, but the resulting unit will not accept SCSI commands.

Secure Path Discovers Unconfigured LUNS

Secure Path configures and displays LUNs that have not been configured under the Solution Software. Delete the connections on the array and reboot the HSG controller to ensure that the connections are offline before proceeding.

Deleting LUNs

Don't delete all LUNs on a storage system. This can result in the Secure Path drivers being unable to communicate with the storage system.

Stop I/O during Spconfig

Make sure that all I/O to the RAID storage systems being configured is stopped before running spconfig. If I/O is running spconfig may fail during the configuration process. If this occurs, make sure all I/O is stopped and rerun spconfig.

Spmgr Notes

- Since spmgr uses TCP/IP sockets for communication with spagent, network services must be configured and functioning properly for spmgr to start. However, this does not effect the failover capabilities of the Secure Path drivers.
- Rebooting with a known failed path results in losing all knowledge of that path. For example, start with an initial condition of 4 paths to a LUN with 3 alive and 1 dead paths, as seen with spmgr display. Reboot the system. Spmgr display then sees only 3 alive paths. A subsequent repair of the path allows *spmgr* to again find the path but spmgr notify has no record of a "repair" event.
- If a preferred path to a device is in the failed state and you issue a spmgr restore -d <device>, the command line responds with a prompt (no apparent response). The path remains in a failed state and no path change is made. This is the expected response to the command.
- The spmgr alias command is used to reference a large cumbersome old_name with a shorter or clearer alias_name. Reversing the argument order such as "spmgr alias old_name alias_name " results in the alias_name replacing the old_name such that any command using the old_name results in error. The alias must then be deleted for the old_name to again work correctly.

- The spmgr alias command checks a table of reserved words to protect you from aliasing words that would result in unexpected behavior. This list is, however, not a comprehensive list. Take precautions to avoid using special characters that could be misinterpreted by the shell such as a leading "-" or "$".

  The current list of reserved words maintained by spmgr is:

add	alias	client	delete	display	help	log
notify	on	off	password	prefer	quiesce	restart
restore	select	set	spmgr	unalias	unprefer	

- The *spmgr quiesce* command has an undocumented option that should be avoided. Do not use spmgr quiesce -d device. This option will quiesce all paths to the specified device and make that device unavailable. As a result, spmgr display -d device results in an "invalid LUN" response and spmgr restart -d device does not work. If this option is inadvertently used, the device can be restarted with the spmgr restart all command.

Documentation Notes

The following are changes to the *Compaq SANworks Secure Path Version 3.0 for Sun Solaris Installation Guide.*

- Page 5-5, step c: The upgrade CDROM will require a different directory path:

  *# cd /*cdrom/sp_v30_sun_upg/solaris

- Page 5-6, step 6a: Add the following text to the end of the step: "Use the CLI to verify that the new ports are in Fabric mode and the connection is online before proceeding."
- Page 5-6, step 6d: Add the following steps between step d and step e.

  a. Select option 3. If the system scan picks up any adapters that you do not want under Secure Path control, delete them before proceeding.

  b. Choose option 4. Modify an Adapter. Option 4 ensures that the adapters discovered in the previous step are properly configured.

NOTE: This step must be performed for every adapter that is being added.

  c. Select an adapter

  d. Answer all the prompts, accepting the default responses.

NOTE: During this step you may change the target numbers and or WWPNs for your specific configuration, if desired.

- Page 5-6, step 6e: Add this to the end of the step: “Ignore any error messages that are displayed during reboot.” These will include:

  Error retreiving data

NOTE: In the previous error message the word retrieving is spelled incorrectly. This will be fixed in a later release.

  /etc/rcS.d/S65spinit Cannot find storage, reconfiguration in progress

  /etc/rc2.d/S89spinit Cannot find swsp devices, reconfiguration in progress

- Page 5-6, step 7: The filename /opt/CPQswsp/devices.xref is wrong, it should be /opt/CPQswsp/device.xref.

Third Party Software

Veritas software supported

The following Veritas software is supported with Secure Path 3.0 under Solaris 2.6, 2.7 and 2.8:

- VXFS, version 3.3.3
- VM, version 3.1.1
- VCS, version 1.3

Disabling DMP on VERITAS Volume Manager versions prior to version 3.1.1

To disable the DMP driver in VERITAS Volume Manager (VxVM) prior to version 3.1.1, use the following steps:

1. Unmount all file systems created on Volume Manager volumes with the following command:

   unmount

2. Stop the Volume Manager. Type:

   vxdctl stop

3. Remove the "vxdmp" driver from the "/kernel/drv" directory. Follow both commands in the order shown as follows:

   rm /kernel/drv/vxdmp

   mv /kernel/drv/sparcv9/vxdmp /kernel/drv/sparcv9/vxdmp.SunOS.'uname -r'

4. Edit /etc/system and remove the line:

   forceload: drv/vxdmp

5. Remove the Volume Manager DMP files:

   rm -rf /dev/vx/dmp /dev/vx/rdmp

6. Link /dev/vx/dmp to /dev/dsk symbolically:

   ln -s /dev/dsk /dev/vx/dmp

7. Link /dev/vx/rdmp to /dev/rdsk symbolically:

   ln -s /dev/rdsk /dev/vx/rdmp

8. Shut down the system to disable the DMP functionality:

   /usr/sbin/shutdown

NOTE: DMP must stay loaded on versions 3.1.1 and above.

Disabling DMP on VERITAS Volume Manager Version 3.1.1 and later

To disable the DMP driver in VERITAS Volume Manager (VxVM) version 3.1.1 and later, use the following steps:

1. Launch the vx disk administrator with the following command:

   vxdiskadm

2. Choose option 17 - Prevent multipathing/Suppress devices from VxVM's view.
3. Type y at the prompt to continue.
4. Choose option 5 - Prevent multipathing of all disks on a controller by VxVM.
5. Type list to view controllers that Volume Manager has access to.
6. Enter the controllers that are being used by Secure Path. For example, choose c7 to exclude all LUNs on c7 from DMP control.
7. Type q to quit from the DMP administrator.
8. Type q to quit from the vx disk administrator.

Sun Cluster 2.2 and 3.0

Sun Cluster 2.2 07/00 release is supported on Solaris 2.6, 2.7, and 2.8. Sun Cluster 3.0 is not supported in this release.

Failover Time Running DRM

Failover time in /kernel/drv/fca*.conf file doesn't account for scsi timeout value. If running DRM, you will have to increase failover time in /kernel/drv/fca*.conf file. Refer to DRM documentation for specific instructions.

Updating an Existing SWCC Access Device During Secure Path Installation

1. Exit any SWCC Client session that you have running for this host and stop the SWCC Agent by running /opt/steam/bin/config.sh.

   At the menu prompt use the following steps:

   a. Select 3. Start/Stop the Agent.

   b. Select Quit to exit the menu.

2. Mount the Secure Path 3.0 Sun Solaris CDROM using the procedure in the section titled "Installing Secure Path" in Chapter 3 of the *Compaq SANworks Secure Path Version 3.0 for Sun Solaris Installation and Reference Guide*.

3. Refer to the *Compaq SANworks Secure Path Version 3.0 for Sun Solaris Installation and Reference Guide* to install Secure Path.

4. Use format to identify a new SWCC access device in the form of /dev/dsk/c#d#t#s2 after Secure path has been installed and the system has rebooted. For the example in the next step, assume that the new SWCC access device is c10t0d0s2.

5. Run /opt/steam/bin/config.sh to Modify the old SWCC access device to the new access device. Use the following steps:

   a. Choose option 15. Modify a Subsystem.

   b. Enter the position number of the subsystem you wish to modify.

   c. Choose option 2. Access device.

   d. Enter the new access device in the form of cXtYdZs2.

   e. Enter D to exit if your information is correct. Choose N if there are no other systems to modify, otherwise repeat steps b-e until all modifications are made.

   f. Choose E to exit and save system changes.

g. Choose option 3. Start/Stop the Agent. If the agent is running, stop it and then restart it. If the agent is not running, start it.

Configuring SWCC Agent Failover within a Clustered Environment

Compaq recommends that when you set up SWCC agent monitoring in a clustered environment, you should configure monitoring through a logical host instead of through a physical host. This allows SWCC to continue to operate throughout failovers in the cluster. To configure SWCC to failover within a cluster, use the following steps on all nodes in the cluster that can master the logical host that will be used for failover:

1. Launch the configuration utility:

   /opt/steam/bin/config.sh

2. Choose option 13. Add a Subsystem and then option 1. Automatic Scan. Choose the appropriate arrays to be under SWCC control and enter the appropriate information as prompted. Enter quit to return to the main menu.
3. Choose option 17. Add a Client. Option 17 is used to enter the host name of the SWCC client, access level and error notification level. Verify the information entered is correct and enter quit to return to the main menu.
4. Choose option 3. Start/Stop the Agent. Start the agent if it is currently not running. Stop and then restart the agent if it is already running.

Use the following steps on the SWCC Client system only:

1. Launch the SWCC agent GUI.
2. Under the File menu, choose Add System.
3. Enter the TPC/IP Address of the logical host in the cluster that the SWCC client system will gain access through and click “apply” and then “close”.

Troubleshooting Secure Path

Table 4 defines the way that an "Event" such as a failure or state change is reported to the server through the Secure Path driver (hsx) or agent (spagent). The Response Action column shows where the event is logged. LOG is the */var/adm/syslog/messages* file, CONSOLE is the root console and NOTIFY is email notification. The Level column indicates the criticality of the event and is used by the Secure Path Manager (*spmgr*) to allow the system administrator to route events to specific users. The levels are further defined in the *Compaq Secure Path Version 3.0 for Sun Solaris Installation and Reference Guide.*

Table 4: Responses and Severity Level for Supported Events

Event	Response Action	Level
Path failed	LOG+CONSOLE+NOTIFY	WARNING
Failover condition detected	LOG+CONSOLE+NOTIFY	CRITICAL
Failover start	LOG+CONSOLE+NOTIFY	INFORMATIONAL
Failover complete	LOG+CONSOLE+NOTIFY	INFORMATIONAL
Restore start	LOG+CONSOLE+NOTIFY	INFORMATIONAL
Restore complete	LOG+CONSOLE+NOTIFY	INFORMATIONAL
Restore failed	LOG+CONSOLE+NOTIFY	INFORMATIONAL
Excessive restores	LOG+CONSOLE+NOTIFY	WARNING - auto restore has been disabled until next time quantum (1 hour)
Availability Changed	LOG+CONSOLE+NOTIFY	CRITICAL
Select Complete	LOG+CONSOLE+NOTIFY	INFORMATIONAL
Select Failed	LOG+CONSOLE+NOTIFY	WARNING
Unit Attention	LOG	INFORMATIONAL
Select Start	LOG +CONSOLE+NOTIFY	INFORMATIONAL