SANworks by Compaq

Release Notes –
Data Replication Manager
HSG80 ACS Version 8.6-4P

Part Number: AA-RPJ2C-TE

Third Edition (February 2002)

Product Version: ACS Version 8.6-4P

This document provides information for *SANworks*^{TM} Data Replication Manager by Compaq (operating with HSG80 Array Controller Software Version 8.6-4P) that is not covered elsewhere in the documentation. Individuals responsible for configuring, installing, and using the Data Replication Manager solution should use this document.

For the latest version of these Release Notes and other Data Replication Manager documentation, visit the Compaq storage website at:

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

COMPAQ

Release Notes Contents

These release notes cover the following major topics:

Intended Audience

This document is intended for customers who purchased or upgraded to *Compaq StorageWorks*™ Data Replication Manager HSG80 Array Controller Software Version 8.6-4P, and for Compaq authorized service providers responsible for installing, configuring, and maintaining DRM systems.

What's New

Compaq Array Controller Software (ACS) Version 8.6-4P contains new features that expand upon the capabilities of Version 8.5P. The following sections summarize the major new features, enhancements, and requirements of Version 8.6-4P.

NOTE: Although the current version of ACS software is 8.6-4P, Compaq supports all patch versions of 8.6P software. Current software updates and patches can be found at:

http://www.compaq.com/products/storageworks/softwaredrivers/acs/index.html

Customers are encouraged to install the patches for their specific content as required.

Heterogeneous Open SAN Environment

Compaq's heterogeneous Open SANs now support a wide range of multi-vendor hardware platforms and operating systems in a mixed environment. This allows users to tailor their SANs for the specific platforms and operating systems they require. With Version 8.6-4P, Compaq storage controllers can be shared across many different platforms and operating systems, all managed within the same SAN.

To share storage, all hosts must be multi-bus failover enabled, and they must share the same SCSI mode.

Specific support limits and interoperability of individual platforms and operating systems may vary, and need to be understood and considered when evaluating SAN designs. Refer to the *Compaq StorageWorks Heterogeneous Open SAN Design Reference Guide* (part number AA-RMPNC-TE) for SAN design guidance.

Additional information on DRM rules and design guidelines can be found in the *Compaq Features and Benefits of ACS 8.6P Data Replication Manager* white paper (part number 1653-1202A-WWEN), and the *SANworks by Compaq Application Notes - HSG80 ACS 8.6-4P Data Replication Manager Design Guide* (part number AA-RQ78A-TE).

Supported Operating Systems

ACS Version 8.6-4P supports the following operating systems:

- *Compaq OpenVMS*™
- *Compaq Tru64*™ UNIX
- Hewlett-Packard HP-UX
- IBM AIX
- Microsoft Windows 2000 (Server, Advanced Server, Datacenter)
- Microsoft Windows NT
- Novell NetWare
- Sun Solaris

Switch Configurations

There is a restriction in DRM design options when building Fibre Channel fabrics using Compaq Fibre Channel switches by Brocade and running the currently supported Brocade switch firmware and ACS Version 8.6-4P. These limitations are as follows:

- A maximum of 7 hops from server to storage controller (HBA to controller port 1),

- A maximum of 7 hops from initiator storage controller to target storage controller (port 2 to port 2),

- A maximum of 20 switches per fabric, split between the two sites.

There are several unique cases that are supported but do not follow this rule. For example, in a basic DRM configuration, there is only one switch per fabric at each of the two sites. This configuration is supported. Also, the optional entry-level DRM solutions offered in Chapter 5 of the *SANworks by Compaq Data Replication Manager HSG80 ACS Version 8.6-4P Configuration Guide* do not follow this rule.

The *Compaq StorageWorks Heterogeneous Open SAN Design Reference Guide* is available on the web at:

http://www.compaq.com/products/storageworks/san/documentation.html

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.

Fibre Channel SAN Switch V2.6 Firmware Compatibility with DRM

Fibre Channel SAN Switch V2.6 firmware supports DRM in all configurations, with the following exceptions:

- DRM solutions using the Novell operating system are not currently supported by Fibre Channel SAN Switch V2.6 firmware, and will require the use of earlier firmware versions. Please reference the DRM software support matrix for the latest information on Novell. This matrix can be found at:

  http://www.compaq.com/products/sanworks/drm/softwaresupport.html.

- Fibre Channel SAN Switch V2.6 firmware supports DRM using Fiber Channel (FC) optical links, and links through wavelength division multiplexing (WDM) boxes that do not alter the FC protocol. It does not currently support some DRM configurations using FC-IP or FC-ATM links, and will require the use of earlier firmware versions. For the latest update on supported DRM configurations please refer to the DRM Application Notes for intersite links, which can be found at:

  http://www.compaq.com/products/sanworks/drm/documentation.html.

Table 1 and Table 2 summarize this information.

Table 1: DRM SAN Switch Firmware Support Matrix

Operating System	Firmware V2.1.9m	Firmware V2.6
Compaq Open VMS		X
Compaq Tru64 UNIX		X
HP-UX		X
IBM AIX		X
Novell NetWare	X	
Microsoft Windows 2000		X
Microsoft NT		X
Sun Solaris		X

Table 2: Switch Firmware Required by Network Interconnect Gateway

Network Interface	Firmware V2.1.9m	Firmware V2.4.1
CNT IP	X	
San Valley	X	
San Castle		X

NOTE: Novell NetWare is the restriction for FC SAN switch firmware version. As shown in Table 1, if a Novell server is in the SAN, then the lower version switch firmware must be used for all switches.

NOTE: If there is a conflict in which version of the FC SAN switch firmware to use based on either Table 1 or Table 2, Table 2 will take precedence.

Rolling Upgrade

The rolling upgrade procedure is documented in the *SANworks by Compaq Data Replication Manager HSG80 ACS Version 8.6-4P Configuration Guide*. The procedure is designed to allow an array controller software upgrade without the need for a server reboot. However, you must ensure that all the latest drivers, and if applicable, the latest release of Secure Path are installed prior to this upgrade. Installing the latest drivers may require the server to be rebooted. Information on the latest supported drivers and Secure Path can be found in the Software Support Matrix at:

http://www.compaq.com/products/sanworks/drm/softwaresupport.html.

Scripting

Scripting for automated failover and failback procedures are supported for Windows 2000/NT, Compaq OpenVMS, Compaq Tru64 UNIX, IBM AIX, and Sun Solaris operating systems. For more information on automated procedures, refer to the *Compaq SANworks Data Replication Manager HSG80 ACS Version 8.6-1P Scripting User's Guide.* For manual procedures, refer to the *Compaq SANworks Data Replication Manager HSG80 ACS Version 8.6-4P Failover/Failback Procedures Guide*.

Common Platform Issues

Performance Considerations—Adding Target Unit Back to Remote Copy Sets

When you add back the target unit to the remote copy sets with the following command,

```
SET RemoteCopySetName ADD = TargetRemoteCopyName\UnitName

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

it forces each remote copy set into a full normalization. In some cases this will have an impact on data replication performance and, as such, should not be performed during periods of high target site I/O activity. You may wish to stagger the startup of the normalization of each remote copy set to minimize the performance impact.

Performance Considerations—Full Copy Operation

During full copy operations, host I/O performance will be moderately reduced, and the length of time required for the copy operation will be longer than that for a merge operation.

Performance Considerations—Write History Log Merge

During Write History Log merge, host I/O performance will be drastically reduced due to the high priority given to the merge operation. The length of time required for the merge operation will not be affected by host I/O.

SWCC and SANworks Management Appliance Limitations

The HSG80 controller does not distinguish between commands issued from in-band command tools (SWCC, Command Scripter, and *SANworks* Management Appliance) and commands issued out-of-band through the serial port. Serial port commands should only be performed when the customer has restricted commanding from other sources. Special care must be taken with the Management Appliance, as it periodically issues polling commands that can interrupt serial port communications. If you will be using the serial port on the HSG80 controller, remove the Management Appliance from the fabric or use switch zoning to isolate the Management Appliance from the array in which controllers are commanded through a serial port.

Future releases of Management Appliance and ACS firmware will contain enhancements to prevent this inconvenience.

Using Switch Zoning to Prevent Crashes When Using VTDPY Host Display

The HSG80 controller may crash when using the Display Host functionality in VTDPY. If more than 21 connections are displayed (the equivalent of one page), the controller will crash with a last fail code of 01932588 (cache data allocation parity error). Compaq recommends that you use switch zoning to limit the number of connections visible to the controller. For more information about switch zoning, refer to the *SANworks by Compaq Data Replication Manager HSG80 ACS Version 8.6-4P Configuration Guide*.

Resetting FcAL fanFrameDisable Value to Zero

If you perform a CONFIGURE command and change the setting of any of the Fabric Parameters, the value of the FcAL fanFrameDisable parameter also becomes changed from 0 to 1. You must go into the Arbitrated Loop Parameters and change the setting of Send FANframes to 1. This will reset the FcAL fanFrameDisable parameter back to 0. When you have made this change, perform a CONFIGSHOW command to verify that FcAL fanFrameDisable parameter is at 0.

Failure to reset Send FANframes to 1 may impact the proper functioning of a fabric failover if you have an HBA with an arbitrated loop setting.

Invalid VTDPY Percentages

During the transition time between site failover and site failback, the log, merge, and copy percentages on the original initiator displayed by VTDPY are not valid. Disregard these percentages.

Using Switch Zoning to Prevent Crashes When the 96-Connection Limit is Exceeded

The HSG80 controller may crash if more than 96 connections exist on the fabric. Compaq suggests that you use switch zoning to limit the number of connections visible to the controller. For more information about switch zoning, refer to the *SANworks by Compaq Data Replication Manager HSG80 ACS Version 8.6-4P Configuration Guide*.

I/O Pause During Fabric Reconfiguration

During a fabric reconfiguration, you will notice a brief pause in I/O functions on all servers connected to the fabric. This brief cessation of read/write operations is normal. Fabric reconfiguration can be caused by switches starting up or shutting down, and by the physical plugging or unplugging of fiber cables.

Controller Saturation

High usage of many remote copy set and non-remote copy set LUNs will have a serious impact on the performance of the remote copy set LUNs, causing controller saturation and possibly starving a full copy operation.

A saturated controller condition begins approximately when idle time falls to 25% or less. When this occurs, you may see Aborted Command errors through the Command Line Interface (CLI).

To prevent controller saturation:

- Avoid placing multiple heavy use loads on the controllers.

- Use the VTDPY screen to monitor controller idle time percentage. Adjust load accordingly to maintain an idle time of 25% or greater.

RAID 5 Remote Copy Set Target Drop

RAID 5 remote copy set targets may be dropped under the following combined conditions:

- No write history log disk is configured, and

- Host I/O is accessing the initiator remote copy set LUNs.

When both target controllers are shut down, a full copy operation will be triggered. When the target controllers are restarted, they will begin a 3-minute memory diagnostic.

While the memory diagnostics are running, the full copy I/O to RAID 5 target LUNs will be stalled. Therefore, after approximately 2 minutes, a timeout will occur and the target LUNs will be dropped from the remote copy set. This target drop problem occurs only on RAID 5 remote copy set LUNs.

Remedies:

- To prevent target LUN drop, before target controllers are booted or powered on, set port_2_topology on both initiator controllers to *offline*. Wait 5 minutes after target controllers are restarted to allow for memory diagnostics to complete before setting port_2_topology on the initiator controllers back to *fabric*.

- If the target LUNs are dropped, wait 5 minutes to allow for the target controller memory diagnostics to complete, then add the targets back into the remote copy sets. The full copy operation will begin.

Required Delay Time Before Failback

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.

Removing Targets from the Proper Controller

A problem occurs if both fabric intersite links are not functioning and you remove the target of a remote copy set that is part of an association set that has a write history log. If you issue the command to remove the target from the opposite controller that the remote copy set is not on line to, and then issue the CLI command SHOW REMOTE COPY SET FULL, the target state will indicate LUN D0 is copying 0% complete. The actual indication of the target state should be "No targets."

Example:

```
Name                                           Uses            Used by
--------------------------------------------------------------------------
RCS1           remote copy                       D1              AS1
        Reported LUN ID: 6000-1FE1-0007-9DD0-0009-0510-3907-000E
        Switches:
          OPERATION_MODE  = SYNCHRONOUS
          ERROR_MODE      = NORMAL
          FAILOVER_MODE   = MANUAL
          OUTSTANDING_IOS = 20
        Initiator (BUILDNGA\D1) state:
          ONLINE to the other controller
        Target state:
          \D0             is COPYING                 0% complete
```

The real problem occurs when you try to add the target back in, at which time you will see the %EVL error message: "Too many targets have been specified in this set."

Solution: You cannot add a target if you are in a normal production mode or if you are in a failed over condition. You must first issue the CLI command to delete the remote copy set, and then issue the CLI command to add the remote copy set back in. Deleting and then re-adding the remote copy set will force normalization.

Startup of Only One Fabric at a Time

When an event occurs that causes a fabric reconfiguration (for example, a scheduled or unscheduled outage of intersite links, addition or removal of a switch or switch-to-switch link, and so on), you should allow all of the Fibre Channel switches in that fabric to reconfigure, before you reconfigure the second fabric.

Intermittent Double Normalization After a Full Failback or Failback To New Hardware Procedure

After you have performed a full failback or failback to new hardware, a second normalization (from the initiator to target) can occur. This double normalization happens after the point in the failback procedure where you add the target and normalize your storage sets (from the target to initiator).

The only effect of this extra normalization is to add the additional controller overhead of doing a full copy—it causes no data corruption. When normalization is complete, you can proceed with the failback and add the load at the appropriate point in the procedure.

Command Scripter Communication Loss Due To SCSI Error

If Command Scripter v1.0 has a loss of communication while a script is running, it will cause the script to abort, and the script will not finish running. You must then put the controllers in a known state by issuing the appropriate CLI commands from the controllers. You can examine the .log files in the $CLONE_HOME/log directory to determine which commands had been executed before communication was lost.

If the communication failure is due to a SCSI error, then the loss of connection is only momentary. You can verify that the connection is re-established by issuing the following command from the host:

```
cmdscript -f <device Name> "show this"
```

However, if this command continuously gives a communication failure error, a hardware failure or configuration error is indicated. You will need to troubleshoot the loss of connection for causes such as broken links, failed devices, controller configuration, and so on.

Waiting for Write History Logging Disks

After clearing invalid cache and lost data, remote copy set processing will halt. When you issue the CLI command, SHOW REMOTE_COPY_SETS FULL, if you see the following error message:

```
Waiting for write history logging disks to become ready.
```

restart the controller to clear this condition.

Association Sets

Association sets can contain up to 12 remote copy sets. However, because all copy sets within an association set are moved between controllers as a group, all remote copy sets within an association set must be accessed by the same server.

For instance, 6 remote copy sets (one association set) could be accessed by one server and 6 remote copy sets (another association set) by the other.

Platform-Specific Issues

Compaq OpenVMS

Additional Software Requirements

A list of the most current software for Compaq OpenVMS can be found at the following website:

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

Follow the Software Support Matrices link, then choose OpenVMS.

Remedial kits that you may require are available at:

http://www.openvms.compaq.com/openvms/fibre

Platform-Specific Issues

There are no platform-specific issues for OpenVMS.

Compaq TRU64 UNIX

Additional Software Requirements

A list of the most current software for Compaq Tru64 UNIX can be found at the following website:

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

Follow the Software Support Matrices link, then choose Tru64 UNIX.

Prevent Possible Data Corruption

If during the failover procedure you are unable to stop all applications and dismount all units that are part of a remote copy set, you must reboot hosts prior to failback. This prevents possible data corruption caused by writing stale data from host cache to the units after failback.

NOTE: Extreme care must be used when creating and managing remote copy sets on an ATM link. If these links are overstressed (for example, an excessive number of remote copy sets created for a given environment), unexpected behavior may result, such as loss of remote copy sets and link failures.

Command Scripter Communication Failure Error

If the original path to the command console LUN (CCL) is lost, then Command Scripter will give a communication failure error. You will need to reboot the host to establish the second path to the CCL.

Hewlett-Packard HP-UX

Additional Software Requirements

A list of the most current software for HP-UX can be found at the following website:

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

Follow the Software Support Matrices link, then choose HP-UX.

Failure to Mount File System after Failover or Failback

If you are unable to mount a previously configured file system after a failover or failback, run fsck on the logical volume and retry the mount.

Configuring Host Server Remote Copy Sets

Remote copy sets (RCS) at the target site will acquire the world wide name of their RCS at the initiator site when a failover occurs. Compaq recommends that you not configure the RCS on the HP-UX host servers at the target site until after a failover.

IBM AIX

Additional Software Requirements

A list of the most current software for IBM AIX can be found at the following website:

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

Follow the Software Support Matrices link, then choose IBM AIX.

Microsoft Windows 2000

Additional Software Requirements

A list of the most current software for Windows 2000 can be found at the following website:

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

Follow the Software Support Matrices link, then choose Windows 2000.

Auto Failback

The Secure Path for Windows 2000 Auto Failback feature is not currently supported in a Data Replication Manager configuration. Disable this feature by starting Secure Path Manager, then selecting **Properties** > **Autofailback** > **Disable**.

Booting Windows 2000 Servers Over the Fabric

Any of the Windows servers can be booted from a LUN on an HSG80 controller, including a LUN that is part of a remote copy set. Instructions for configuring servers and installing Windows 2000 are available on the Web at:

http://www.compaq.com/support/storage/open_vendor/support/RAIDarray/boot_support_external_web.html

Two problem situations could arise when booting over the fabric:

- If the boot LUN is online to a controller that the server cannot access, the server will be unable to boot. This condition could occur if the link between the server and the fabric is broken. At this stage of booting, the server cannot move the LUN between controllers. The LUN must be manually moved to the other controller by issuing a RESTART THIS_CONTROLLER CLI command.

- When an intersite link with high latency (such as ATM) is used, the server may take a long time to boot, and may be slow to respond during normal operation. This is normal behavior for the server. It is caused by the time required to replicate the boot disk across a very long distance.

Check Status

If a target controller or switch becomes inoperative and the Windows 2000 host is rebooted, Secure Path Manager will not provide a report informing you that you have lost multipath capability.

If you attempt to move a LUN to the inoperative path, a warning message appears, indicating that you should check the Application Event Log for details. This may be an indication that you have lost multipath capability.

Check the status of links, target switches, and target controllers.

HSG80 Controller Soft Shutdown/Restart

When the SHUTDOWN THIS or SHUTDOWN OTHER command is executed from the CLI, the controller will shut down, forcing the LUNs to change paths. Secure Path will immediately fail the LUNs over to the remaining path, but the original path may not be marked as failed for several minutes.

Similarly, when the RESTART THIS or RESTART OTHER command is executed from the CLI, the controller will restart, forcing the LUNs to change paths. Secure Path will immediately fail the LUNs over to the remaining path, but the original path will never be marked as failed. The icon for the failed LUN will be marked with a yellow triangle with an exclamation point inside. The controller will finish restarting and return to normal operation without notification.

The following procedure can be used to check whether a system is in this state:

1. Select one of the units in Secure Path Manager.

2. In the right-hand pane, click the path marked **Available**, and then right-click it to bring up the menu.

3. Select **Verify Path** from the menu that appears.

If the verify fails, the path is not available. The path becomes available again after the controller is booted.

Component failures and other real failure scenarios cause paths in Secure Path to be correctly marked as failed.

LUNs Numbered Incorrectly

When LUNs are moved between hosts (such as during a site failover or a site failback), it is possible that the LUNs may become "out of letter order."

To prevent the "out of letter order" status, before booting the Windows 2000 host, follow the steps below:

1. Make sure all LUNs are failed over to one HSG80 path. From the HSG80 CLI prompt, issue the following command:

   ```
   Restart Other_Controller
   ```

2. Use Disk Manager to assign the correct drive letter so that the disks now match the units on the controller.

3. Once Windows 2000 sees the disks ordered properly, use Secure Path Manager to move the units to the correct path.

Changing Host Connection Unit Offsets

If the UNIT_OFFSET of a connection is changed, the host must be rebooted to recognize the change. The host will continue to operate using the offset that was previously in effect until it is rebooted. For example, if a host connection has a unit offset of zero, it will be able to access only units D0 through D7. If the offset is changed to 8, the host will still be able to access units D0 through D7 until it is rebooted. After reboot, it will be able to access only units D8 through D15.

Windows 2000 Plug and Play Manager Generates Numerous Pop-up Windows

Each time a LUN is dismounted ungracefully (for example a fabric failure), Windows 2000 displays a pop-up window that warns of "Unsafe removal of device." This window can be cleared by simply clicking **OK**. The window itself is harmless, but additional dismounts cause more pop-up windows to appear. These windows can stack up on the desktop and consume memory to the point that the system crashes. However, several hundred dismounts and associated pop-up messages are required before a system crash is probable.

Windows Using Large LUNs While in SCSI-2 Mode

DRM supports Windows 2000 hosts accessing LUNs above D7 without offsets via large LUNs. However, all hosts using large LUNs to access LUNs on a controller in SCSI-2 mode must be able to access LUN D0. Refer to the *Compaq SANworks Secure Path Version 3.1 for Windows Installation and Reference Guide* for additional information.

Association Sets

In a Windows 2000 cluster configuration, all remote copy sets within an association set must be placed in one cluster resource group.

Microsoft Windows NT

Additional Software Requirements

A list of the most current software for Windows NT can be found at the following website:

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

Follow the Software Support Matrices link, then choose Windows NT.

Auto Failback

The Secure Path for Windows NT Auto Failback feature is not currently supported in a Data Replication Manager configuration. Disable this feature by starting Secure Path Manager, then selecting **Properties** > **Autofailback** > **Disable**.

LUNs Numbered Incorrectly

When LUNs are moved between hosts (such as during a site failover or a site failback), it is possible that the LUNs may become "out of letter order."

To prevent the "out of letter order" status, before booting the Windows NT-X86 host, follow the steps below:

1. Make sure all LUNs are failed over to one HSG80 path. From the HSG80 CLI prompt, issue the following command:

       Restart Other_Controller

2. Use Disk Administrator to assign the correct drive letter so that the disks will now match the units on the controller.

3. Once Windows NT sees the disks ordered properly, use Secure Path Manager to move the units to the correct path.

Windows Using Large LUNs While in SCSI-2 Mode

DRM supports Windows NT hosts accessing LUNs above D7 without offsets via large LUNs. However, all hosts using large LUNs to access LUNs on a controller in SCSI-2 mode must be able to access LUN D0. Refer to the *Compaq SANworks Secure Path Version 3.1 for Windows Installation and Reference Guide* for additional information.

Association Sets

In a Windows NT- X86 cluster configuration, all remote copy sets within an association set must be placed in one cluster resource group.

Novell NetWare

Additional Software Requirements

A list of the most current software for Novell NetWare can be found at the following website:

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

Follow the Software Support Matrices link, then choose Novell NetWare.

NetWare Cluster Services (NWCS)

NWCS v1.01 SP1 is supported at the initiator and target sites. Stretch Clusters are not supported at this time. A Stretch Cluster is defined as having a NetWare Cluster using NWCS with cluster members located at both the DRM initiator and target sites. NWCS supports both remote copy set and non-remote copy set LUNs.

Planned Failover/Failback with NWCS

When preparing the initiator and target sites for a planned failover/failback, use caution when removing access to the LUNs at the initiator site. Removing access to the split brain detector (SBD) partition, as well as the cluster volumes, without first bringing down the cluster will result in server abends. To avoid cluster members abending, issue the following command at the system console:

```
CLUSTER DOWN
```

You can also run ULDNCS.NCF at the system console for each cluster member to unload Cluster Services completely.

NetWare 6 Storage Planning Considerations

If you plan on using Novell Storage Services (NSS) logical volumes in a DRM configuration, you should be aware that the nature of Novell's Distributed File Services (DFS) allows you to span an NSS volume across multiple hard disk partitions. This is not desirable in a DRM configuration. Instead, you should maintain a one-to-one relationship among LUNs, remote copy sets, NSS partitions, NSS pools, and NSS logical volumes.

Additional Instructions for Failover/Failback

When NetWare volumes are created at the initiator site, they are inserted into the Novell Directory Services (NDS) tree as servername_volumename (for example, SERVER1_VOL1). After a site failover, the replicated NetWare volumes are still available and can be mounted by any NetWare server at the target site, but the volumes will now take on the new server name (for example, SERVER2_VOL1). In addition, they will not be automatically inserted into NDS, and for traditional NetWare volumes only, they will not maintain the file system permissions established at the initiator site. You MUST perform the following steps the first time failed-over volumes are mounted at the target site:

Traditional NetWare Volumes

1. After failing over to the target site and mounting the NetWare volumes, type `nwconfig` from the file server console.

2. Select **Directory Options**.

3. Select **Upgrade Mounted Volumes into the Directory**, and supply an administrator-equivalent userid and password.

4. From a Windows workstation (or the File Server's Graphical Console), use the **ConsoleOne** utility to establish the desired file system permissions for the newly inserted volumes.

NSS Logical Volumes

1. After failing over to the target site and mounting the NSS logical volumes, run ConsoleOne from a Windows workstation or the File Server's Graphical Console.

2. From the **Tools** menu, select **Disk Management > NSS Pools**.

3. Select the correct **NDS Tree**, **NDS Context**, and **Server** when prompted.

4. Ensure the **Media** tab is highlighted and **NSS Pools** is displayed. Click the correct **NSS Pool** from the list on the left to highlight the pool, and then click the **Update NDS** button.

5. Click the **Media** tab and then **NSS Logical Volumes**.

6. Click the correct **NSS Logical Volume** from the list on the left to highlight the volume, and then click the **Update NDS** button.

NOTE: You must perform steps 4-6 above for each NSS Pool/Volume pair you failover from the initiator site.

Once the above procedures have been accomplished, they will not have to be performed again as long as the volumes are always mounted on the same target file server after a failover.

Upon failback to the initiator site, any new files or directories created at the target site will need to have permissions reestablished using the ConsoleOne utility (for Traditional NetWare volumes only). When performing subsequent failovers, it is not necessary to insert the volumes into the NDS tree - they will already be there. Simply make sure that the necessary permissions are granted using ConsoleOne if any new files or directories have been created at the initiator site (for Traditional NetWare volumes only).

CPU Hog Abends

If you experience CPU Hog Server Abends, you may have to adjust the *CPU Hog Timeout Amount* (using *MONITOR.NLM* under the menu parameter *Server Parameters*, *Miscellaneous*) to a lower amount or 0 seconds (disabled).

Auto Failback

Auto Failback is supported using Secure Path for NetWare. Failures involving the target site (extended intersite link failures, target switch failures, target controller failures) cause Secure Path to fail LUNs to their alternate paths. However, Auto Failback to the preferred path may not occur after the link is restored. In these situations, use the Secure Path Manager (GUI) to manually move LUNs back to their preferred paths. Refer to the *Compaq SANWorks Secure Path for Novell Netware Installation and Reference Guide* document for additional details on performing this operation.

Partitioned LUNs

Novell servers cannot handle accessing partitions if another partition on the same physical disk (LUN) is accessed by another operating system. When this happens, the Novell server may lockup. To prevent this from occurring, remove access by the other operating system to the partitions.

Maximum Number of Host Bus Adapters

The maximum number of host bus adapters supported by a Novell host is 4. This is a limitation of Secure Path.

Sun Solaris

Additional Software Requirements

A list of the most current software for Sun Solaris can be found at the following website:

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

Follow the Software Support Matrices link, then choose Sun Solaris.

Platform-Specific Issues

There are no platform-specific issues for Sun Solaris.

Compaq Website

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 under ACS 8.6-4P. Documentation referenced in this document, as well as other Data Replication Manager documentation, can be found at this website.