

release notes

hp StorageWorks NAS b3000 v2

Product Version: 3.2

Second Edition (March 2003)

Part Number: 326189-002

These Release Notes are for the HP StorageWorks NAS b3000 v2 running version 3.2 of the NAS software image. They provide important information not covered in other documents.



© 2003 Hewlett-Packard Company.

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information contained in this document is subject to change without notice.

Compaq Computer Corporation is a wholly-owned subsidiary of Hewlett-Packard Company.

Microsoft®, MS-DOS®, MS Windows®, Windows®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information is provided "as is" without warranty of any kind and is subject to change without notice. The warranties for Hewlett-Packard Company products are set forth in the express limited warranty statements for such products. Nothing herein should be construed as constituting an additional warranty.

NAS b3000 v2 Release Notes
Second Edition (March 2003)
Part Number: 326189-002

Japanese Support for the NAS b3000 v2

The HP StorageWorks NAS b3000 v2 supports Japanese but a conversion process must be completed before running Rapid Startup. To convert the NAS b3000 v2 into Japanese, perform the following steps:

1. Connect a Keyboard, Monitor, and Mouse.
2. Login to the local console using the Administrator account. The password field is left blank.
3. Select the Run command from the Start Menu.
4. Enter the following:
`c:\Compaq\Manage\Conv.vbs`
5. Select Yes to convert the system to Japanese and restart the server.

MSA1000 fails to flash correctly when using a DL380 Based G3

When flashing the firmware on an MSA1000 and using a DL380 G3 as the host, the utility will find the MSA1000 (Modular SAN Array 1000) but will not display the unit name nor will it allow new firmware to be uploaded to that device. HP is working to resolve the issue.

Services for UNIX (SFU)

NFS Performance

NFS performance will increase when changing from the default of synchronous writes to asynchronous writes.

To change from synchronous to asynchronous writes (and vice versa), open the Web UI and click Shares, Sharing Protocols, and choose the NFS Protocol and click Properties. Click the NFS Async/Sync Setting button to toggle between asynchronous and synchronous writes.

Note: After toggling between synchronous and asynchronous writes (and vice versa), the NFS server service must be restarted. Inform all users before restarting the service.

Keep in mind the following when toggling between synchronous and asynchronous writes.

1. When the caching setting for Services for UNIX is set to asynchronous writes (caching on), NFS clients may incorrectly assume that all the writes were safely committed to stable storage, however, the writes were only in the Server for NFS cache.
2. For asynchronous writes: Although Server for NFS informs the NFS client that the data has been safely written to disk, the data is still stored in cache, and is waiting to be written to disk. This might cause file corruption issues if, for example, you lose your power supply to the Server for NFS server while data is still in the cache. At this point, the NFS client assumes that data that was lost was actually safely written to disk.
3. With synchronous writes on (caching off), all write requests are immediately committed to disk before a response is sent. Although synchronous writes on does frequently slow NFS file writes, it does improve the stability and data integrity.



WARNING: Turn asynchronous writes on only if you are willing to risk file corruption if any issue with the Services for UNIX server causes the cache to be lost (for example, if the system shuts down, stops responding, loses its power supply, or experiences other serious issues).

nfsstat -z does not reset the NFS statistical counter

The counters can be cleared manually by stopping and restarting the NFS Server service.

Note: Inform all users before restarting the service.

Cannot assign a client group NFS permissions via the Web UI

When attempting to assign a client group NFS permissions using the Web UI, the following error will occur:

```
The client machine name client_group_name could not be resolved.
```

Assign NFS permission to the client group

Open Terminal Services, open Windows Explorer, and assign the client group its NFS share permissions.

NFS Permissions using the Web UI

When creating an NFS share via the Web UI, if a client permission is assigned that is the same as one for ALL MACHINES, the NFS share will be created with ALL MACHINES no access. The client permission will be implemented correctly.

Example:

If the NFS share permission for ALL MACHINES is read-only and a particular client is also assigned read-only, then ALL MACHINES will be assigned no access. In this situation, only the particular client will be able to access the NFS share as read-only and all other machines will be unable to access the NFS share.

NFS Logging

The maintenance of the NFS log through the web interface to the NAS b3000 v2 does not allow the deletion of the log. The NFS log delete option is located in the Web UI under Maintenance, Logs, NFS Log, and then clicking the Clear button. After clicking the Clear button, a confirmation screen will appear. After clicking OK to confirm the deletion, the following error message will appear:

```
Error: There has been a sharing violation. The source or destination file may be in use.
```

The administrator can delete the log after the Server for NFS service is stopped.

Be aware that this will cause a service interruption to all users trying to access NFS shares on the NAS b3000 v2.

1. Open the Web UI to the NAS b3000 v2.
2. Click **Maintenance>Terminal Services** and log in.

3. Right-click the My Computer icon and choose Manage.
4. Open the Services portion of the management tree.
5. Select and stop the Server for NFS service.
6. You will now be able to delete the log using the web interface as instructed.
7. Start the Server for NFS service.

NFS administrative shares support

SFU does not work with administrative shares in the same fashion as CIFS. By default, a volume drive such as C: is CIFS shared as C\$. This is an example of an administrative share and is hidden to CIFS clients. If an NFS share is created and named driveS, as in the example, the share will not be hidden to NFS clients. This NFS share will act as a normal NFS share.

Admin cannot list and map domain users and groups for SFU mapping unless the SFU admin is logged into the domain

The admin must log into the domain before mapping domain users and groups. If the admin is not logged into the domain, then the domain user or group is not on the list Windows users or groups and cannot be mapped.

Volume Mount Points support

Attempting to create an NFS share on a disk mounted on a mount point will result in the error:

```
Cannot write IOCTL to NFS driver...
```

The HP StorageWorks NAS b3000 v2 supports many network sharing protocols including the NFS protocol for UNIX and Linux clients. Shares for which the NFS protocol will be enabled must be created on logical disks that are mounted on a drive letter. Microsoft Windows Powered OS supports mounting virtual disks onto mount points or reparse points created on another disk already mounted on a drive letter.

Mount points enable the administrator to mount many disk devices under a single drive letter, creating the appearance and behavior of a larger disk drive with a contiguous namespace. However, the Microsoft Services for UNIX (SFU) NFS Server does not yet support the functionality of mount points.

All logical disks to be used for NFS sharing should be mounted on a drive letter, not on a reparse or mount point. If no NFS shares will be created on a particular logical disk, that virtual disk may be mounted on a mount point instead of a drive letter.

Password Synchronization will not work correctly on a Domain Controller without an Admin UI

The *sfucustom.msi* file located on the NAS b3000 v2 at c:\SFU does not install an Admin UI for password synchronization on a DC.

The Admin UI is used to setup the following:

- Direction of password synchronization
- Encryption Key
- Port Number
- Password Sync retries

- Which UNIX systems to sync with

Note: NFS Authentication Tools and Password Synchronization can be installed separately or together. The instructions follow.

Instructions to install Password Synchronization on the DC by itself (no NFS Authentication Tools):

1. Allow the `c:\WINNT\bin\SFU` directory of the NAS b3000 v2 to be shared.

```
net share SFU=C:\WINNT\bin\SFU
```
2. On the DC, connect to the share:

```
net use Z: \\NAS_machine_name\SFU
```
3. Change directories from the DC to the root of the connected NAS b3000 v2 share.

```
cd /d Z:\
```
4. Run the install program on the DC:

```
OemSetup.msi ADDLOCAL=PasswdSync SFUDIR=C:\SFU  
OEMINSTALL=TRUE SOURCELIST=Z:\ /! *v %temp%\sfusetup.log /q
```
5. Reboot the DC.
The DC will have to be rebooted manually after installing the password synchronization piece in order to run correctly.
6. Run the Admin UI on the DC and setup password synchronization.
7. Click **StartPrograms>Windows Services for Unix>Services for Unix Administration**.

To install NFS Authentication Tools on the DC by itself (no Password Synchronization), use the instructions outlined in the *HP StorageWorks NAS b3000 v2 Administration Guide*.

To install NFS Authentication Tools and Password Synchronization on the DC:

1. Allow the `c:\WINNT\bin\SFU` directory of the NAS b3000 v2 to be shared:

```
net share SFU=C:\WINNT\bin\SFU
```
2. On the DC, connect to the share:

```
net use Z: \\NAS_machine_name\SFU
```
3. Change directories from the DC to the root of the connected NAS b3000 v2 share:

```
cd /d Z:\
```
4. Run the install programs on the DC in the following order:

```
OemSetup.msi ADDLOCAL=NFSServerAuth SFUDIR=c:\SFU  
OEMINSTALL=TRUE SOURCELIST=Z:\ /! *v %temp%\sfusetup.log /q  
OemSetup.msi ADDLOCAL=PasswdSync SFUDIR=c:\SFU  
OEMINSTALL=TRUE SOURCELIST=Z:\ /! *v %temp%\sfusetup.log /q
```
5. Reboot the DC. The DC will have to be rebooted manually after installing the password synchronization piece in order to run correctly.

User name mapping Japanese characters

User name mapping for the network file system (NFS) server does not support Windows or UNIX user names containing Japanese characters.

The name of NFS client groups that are used by the NFS server cannot contain Japanese characters.

Regular users from UNIX/Linux clients cannot change the ownership of a file

The root user is able to perform a `chown` command on any file from anyone to anyone; this is expected. However, a non-root UNIX user cannot `chown` a file. In past versions of Services for UNIX, a regular UNIX user was able to `chown` a file if they were a member of the “Backup Operator” group. Microsoft instituted a design change between Services for UNIX versions to better comply with security. Reasons for not allowing `chown` by a regular user include:

- Preventing users to circumvent disk quotas
- Preventing users running command (scripts) as another user (in conjunction with the `setuid` bit)

Stale NFS file handle on Redhat 7.2 when cluster group is moved or failed

If a Redhat 7.2 client is mounted to an NFS share on the NAS device and a user other than root is connected, the mount will report `Stale NFS file handle` if the cluster group associated with the NFS share is moved or failed over to the opposite node. To resolve the issue, dismount and remount the share from the Redhat 7.2 client. Upgrading the NFS client to Redhat 7.3 or above resolves the issue as well.

NFS server perflib error in event log/Server for NFS Performance counters are disabled

Server for NFS Performance counters may fail to start. Evidence of the failure is apparent in the event log with multiple NFS server perflib errors. These errors read

```
The Open Procedure for service "NfsSvr" in DLL "C:\SFU\nfs\dsctrs.dll" failed. Performance data for this service will not be available. Status code returned is data DWORD 0.
```

```
Source: Perflib
```

```
ID: 1008
```

The `nfsstat` feature of NFS Server can still be used for Server for NFS counters, but the performance monitor tool of Windows 2000 will not report values. To resolve this issue, the following HP Foundation Agents must be disabled via the Windows 2000 services applet and the NAS device rebooted.

- Compaq Foundation Agents
- Compaq Web Agent
- Compaq Storage Agents
- Compaq Server Agents
- Compaq NIC Agents

To resume HP Foundation Agent support, re-enable the services and reboot the server. Once the HP Foundation Agents are re-enabled, the perflib errors will return.

NFS Permissions in a Cluster

In cluster, NFS client group permissions should be assigned using the Microsoft Cluster Administration tool only versus the Windows Explorer NFS share tab. Permissions assigned outside of the Cluster Administrator will be lost during subsequent failover events or node restarts.

PSM Issues

PSM may fill the event log with inappropriate messages

When cache file space is exhausted, a non-related message is posted to the event log. The message `The driver beneath this one has failed in some way` will appear. This is an indication that the cache file has been exhausted. Increasing the cache size or deleting snapshots will resolve this issue.

PSM creates too large a cache file preventing the volume from being mounted

On large volumes where the cache file percentage is set too high and a snapshot is created, a cache file can get created that is too large for PSM to successfully manage. When this occurs, the drive volume will go offline if the system is rebooted. To avoid this situation, size cache files carefully and in cases where the file gets created inadvertently, shrink the cache size by accessing the volume settings. Should the system get rebooted and the volume is unavailable, a utility named `CleanVol.exe` is available in `c:\winnt\system32\serverappliance`. Run `CleanVol.exe` against the volume in question with `/regfirst` parameter. For example if E: is not mountable, run:

```
cleanvol E: /regfirst
```

A message regarding insufficient resources will be displayed when attempting to access the volume from terminal services or the local console.

PSM supports only 10 TB

PSM support is limited to 10 TB of supported disk space under snapshots even though the NAS b3000 v2 will support larger amounts of storage. There is no built-in mechanism to limit the amount of supported disk space and PSM will not issue any warning when using the product with more than 10 TB. It is highly recommended that snapshots not be used in conjunction with more than 10 TB of space. HP is working with Columbia Data Products to lift this restriction.

Persistent Storage Manager and Scheduling

PSM includes capabilities for scheduling persistent images or snapshots of a selected folder, volume, or group of volumes on a one-time or recurring basis. These schedules are associated with a particular NAS server, so care must be exercised in a NAS cluster to update these schedules whenever cluster disk resources are redistributed due to load balancing or cluster failover activity. After manual load balancing or cluster failovers, the PSM schedule should be checked and updated if necessary. Scheduled items for a particular disk or its member volumes or folders should be deleted from the schedule on their former "preferred owner" cluster node, and recreated on the new owner node. These changes are necessary only if the cluster disk resources will not be moved back to their former "preferred owner" cluster nodes before the schedule item is set to execute.

Persistent Storage Manager and Restoring a Volume

PSM includes the ability to restore a volume from a previously created persistent image. Before initiating a volume restore, notify share users that the volume and any network shares based on the volume will be unavailable during the persistent image restore. During the persistent image restore process, the volume and shares will be taken offline, and Microsoft Cluster service may report cluster physical disk errors. After the restore, the volume will be brought online automatically, but the administrator will need to manually reactivate network shares for the volume.

PSM does not return error message on failed snapshot

When snapshots are taken via the Web UI and failure condition occurs, no information is presented on the web page indicating that the snapshot failed. The user must reference the application and system logs to view if PSM failures have occurred. In addition, the status page for the Web UI, will list out some of the errors PSM may generate when out of boundary conditions are encountered.

NAS Web User Interface

NIC Teaming application generates a C++ Exception Error

Use of the Nic Teaming icons in the control panel and the system tray generate C++ Exception Errors on the NAS b3000 v2 sporadically. Nic Teaming will still function when the error is not generated. Attempt selecting the icon from the control panel again

Unable to select existing quotas for edit and delete

On the quota entry screen of the Web UI, the selection of a particular entry check box is difficult to select. The user must click to the left of the box to select the item.

Improper Closure of Terminal Services

Certain operations such as drive management via ACU can leave the utilities running if the browser is closed versus exiting from the program via the application menu or logging off the terminal server session. In the case of ACU, the drive lights will remain blinking until one of the following occurs:

1. The ACU is accessed again via the link under Disk in the Web UI and the application is closed properly.
2. The orphaned Terminal Server session is closed by Terminal Server and the orphaned application is closed. The default timeout has been set to 15 minutes but it may require up to 30 minutes for ACU to exit. This value may be adjusted in the Terminal Services Configuration Tab under properties of the connection in the HP StorageWorks NAS MMC accessed either through the desktop or via a Terminal Server session.

Other applications may become orphaned in this manner when the Terminal Server Session is exited improperly. Note a maximum of two Terminal Server sessions may be utilized at any given time. Improper exit from a session can result in the sessions becoming consumed. Sessions and processes may be terminated via the Terminal Services Manager via **Start>Programs >administrator tools**.

Configuring NIC Teaming through Terminal Services results in failure of NIC Teaming

When configuring NIC Teaming through Terminal Services, if the port being utilized for access is a part of the NIC Team, NIC Teaming may not install correctly and access to the port may get terminated. It is recommended that either the Remote Insight Lights-Out Edition or local console access is used when setting up the NAS b3000 v2 for NIC Teaming.

Disabled network cards not visible in Web UI

If a network card is disabled, the network card will not appear present in the Web UI. Terminal Services must be used to re-enable the network card before it will be visible again in the Web UI.

Rapid Startup becomes unresponsive

If a NIC Team is established and then Rapid Startup is run with the team in place, the network settings pages will become unresponsive, and the wizard page can not be exited. To exit Rapid Startup, click on some other menu item in the Web UI. Note: NIC Teams will need to be dissolved when utilizing Rapid Startup.

Renaming host does not change address bar of browser

When renaming the host from the Web UI, the server will restart but the address bar identification is not altered. The Web UI may continue to function but may result in The page cannot be displayed message or Terminal Services script error. To correct the issue, type the new name of the server into the address bar.

Renaming host forces a restart where the restart page does not refresh

When renaming the host, or altering the host name in Rapid Start, the restarting page does not refresh to the Welcome page. To resolve the issue, retype the new host name in the address bar on port 3201 or 3202 for secure port access.

Altering the Network interface from DHCP to static causes the page not to return

If the Web UI is utilized to alter the IP settings of the port you are managing from, the host will become unreachable from the current address. When this happens, the network interface page buttons become grayed out and the page does not return, although the settings take affect. To access the Web UI again, close and open the browser and navigate to the newly identified management port.

IP connection metric will not update if Network Port set to DHCP in the Web UI

When the network card is set to DHCP, the IP connection metric will accept a new value and appear to save it, but when the advanced tab of the IP Address Configuration page is revisited, the value is not updated. To update the IP connection metric on DHCP enabled network ports, utilize Terminal Services under the maintenance tab to access the local console navigating to the network and dialup connections from the start menu. The IP connection metric is located under the advance tab of the properties page for Internet Protocol (TCP/IP).

Quota Entries do not appear in the Web UI in the Quota Entries page

Quota Entries may be entered in the New Quota Entry page, but the entries are not displayed in the listing page for the default admin or guest accounts. In addition, if the hostname is altered via the Web UI, quota entries created prior to the rename may not be displayed, see Microsoft Article 328059. To review the quotas entered, access the file system via Terminal Services in the maintenance tab, right click on the volume, select quotas, and quota entries to review the entries listed. Deleting and creating the quotas after a hostname rename will restore the entries.

Terminal Services returns a VBScript error

Terminal Services through the Web UI may cause a VBScript error if the client has a trust violation with the NAS Server. This is caused by the Internet Explorer settings. If you use an IP address instead of using name resolution through a DNS Server, there will be a broken trust issue between the NAS server and the browser. Internet Explorer does not accept ActiveX controls from distrusted web sites.

1. On the client machine, open Internet Explorer 5.5 or higher.
2. From the menu, choose **Tools>Internet Options**.
3. Click the Security tab, select trusted sites, and click the Sites button.
4. Add your NAS server's site to the list of trusted sites and save the settings.

Your ActiveX services should now work.

Managing NTFS Mount points

There is currently no facility for managing NTFS mount points in the Web UI. To create or manage NTFS mount points, you must use Terminal Services. To start terminal services select Maintenance, then Terminal Services on the navigation menu.

System Management Homepage displayed in English

The localization of the System Management Homepage is dependant on the order in which the following services start; Compaq Web Agent, Compaq Foundation Agents, Compaq Version Control Agent, and the Surveyor service. If the System Management Home page is accessed by either browsing to it through the Web UI or accessing it directly at `https://localhost:2381` and it is displayed in English, run the script `C:\Compaq\ElmRestart.vbs` to restart the services in the correct order. This script will stop each of the services listed above and start them in the following order:

- Compaq Web Agent
- Compaq Foundation Agent
- Compaq Version Control Agent
- Surveyor Service

After restarting the above services in the correct order, and restarting your browser, the System Management Homepage will now be properly localized in Japanese.

Default Username and Passwords

The default username and password for administration of the server either through the Web UI or the console is :

```
Username : Administrator
Password : [left blank]
```

The default username and password for the systems management and ACU XE pages of the device are:

```
Username : administrator
Password : administrator
```

DNS settings configured using the Web UI do not take effect immediately

Normally, when adding a DNS server via the standard Windows 2000 console interface from, **Start>Settings>Network&Dialup**, the entry takes effect immediately. When using the Web UI, new DNS entries do not take effect until either one of the following occurs :

- The NIC containing the entry is disabled or enabled using the standard Windows 2000 console interface
- The NAS b3000 v2 is restarted

The Web UI reports the wrong version of the NAS Operating System

While the Quick Restore DVD is labeled as version 3.3, the Web UI reports 3.2. The correct version of the NAS Operating system is 3.3.

NAS DataCopy Cluster Update in the Cluster Install Guide fails

The cluster update utility included in the online Cluster Installation guide fails to properly update NAS Datacopy for cluster awareness. To resolve this issue there are the following workarounds:

1. As it is recommended, install NAS Data Copy AFTER the cluster is completely installed. In this instance the update utility is not required.
2. If NAS Data Copy is installed before clustering the system, the user will need to either un-install/re-install NAS Data Copy or alternatively from the run applet of the start menu, enter the following command:

```
C:\winnt\bin\DataCopy\ClusterUpdate\instclus.cmd
```

This makes NAS DataCopy cluster aware.

System is displayed as a "StorageWorks NAS e7000"

The NAS device will appear as a "StorageWorks NAS e7000" on the HP System Management Homepage and in Rapid Launch, immediately after a Quick Restore of the unit. To resolve this issue, reboot the server. The configuration files will reload and the system will be displayed appropriately.

Web UI continues to display Orphaned Shares

In Windows 2000, deleting a disk that contains a share leaves an orphaned share on the file system. Orphaned shares will continue to be displayed in the Web UI until removed or until the system or service is restarted.

Resolution:

There are three methods to remove orphaned CIFS and NFS shares from the system. Methods one and two cause an interruption in service.

1. Restart the Server service
 - a. Open the web interface to the NAS b3000 v2.
 - b. Click **Maintenance>Terminal Services** and log in.
 - c. Right-click the My Computer icon and choose Manage.
 - d. Open the Services portion of the management tree.
 - e. Select the Server service, right-click, and select restart.
2. Restart the NAS b3000 v2
 - a. Open the web interface
 - b. Browse to **Maintenance>Shutdown>Restart**.
 - c. Click OK to restart the NAS b3000 v2.
3. Or rebuild the share drive and share folder, then remove each share.
 - a. Open the web interface to the NAS b3000 v2.
 - b. Click **Maintenance>Terminal Services** and log in.
 - c. Create a disk and map it to the same drive letter as the orphaned share.
 - d. Recreate the path to the orphaned share.
 - e. Delete the share.

If the orphaned share was also an FTP Share, perform these additional steps:

1. Click the NAS Management console found on the desktop.
2. Expand Core Operating System.
3. Expand Internet Information Services.
4. Expand the NAS machine name.
5. Expand the Default FTP site tab.
6. Right-click the name of the share to delete.
7. Choose delete.

If the orphaned share was also an HTTP Share, perform these additional steps:

1. Click the NAS Management console found on the desktop.
2. Expand Core Operating System.
3. Expand Internet Information Services.
4. Expand the NAS machine name.
5. Expand the Shares tab.
6. Right-click the name of the share to delete.
7. Choose delete.

Microsoft Powered OS

System hangs when using NAS Datacopy on heavily used system

In systems containing less than 2 GB of memory, use of NAS Datacopy in conjunction with large amounts of file share traffic can cause the system to hang. HP recommends that systems exhibiting this behavior be upgraded to 2 GB. This issue will be addressed in a softpaq for the product.

Event Log Messages in the Event Log

During a reboot of the system when services are starting, dependent services may fail initially waiting for other services to start. Messages will get logged to the event log and can be ignored as the service will restart. Messages include services related to:

MSFTPSVC

The description for Event ID (105) in Source (MSFTPSVC) cannot be found. The local computer may not have the necessary registry information or message DLL files to display messages from a remote computer. Refer to Microsoft Knowledge Based Article Q240779.

W3SVC

The description for Event ID (105) in Source (W3SVC) cannot be found. The local computer may not have the necessary registry information or message DLL files to display messages from a remote computer. Refer to Microsoft Knowledge Based Article Q240779.

Userenv

Windows cannot determine the user or computer name. Return value (1722). Refer to Microsoft Knowledge Based Article Q261007.

Perfdisk error

WMI ADAP unable to process PerfDisk performance library due to a time violation in the open function. Refer to Microsoft Knowledge Based Article Q266416.

Application Event Log contains benign error

The following Informational Event will appear in the System Log:

Type: Information Source: Application Popup

Event ID: 26

Description: Application popup: swnas.exe - Application Error. The application failed to initialize properly (0xc0000142).

Click OK to terminate the application.

While the error appears, the HP *swans.exe* utility has executed as designed. The error should be disregarded.

TCPIP Error fills event log

During normal operations of the NAS b3000 v2 TCPIP errors may fill the event log. The event reads as follows.

The collect procedure for the “TCPIP” service in DLL *C:\winnt\system32\perfctr.dll* generated an exception or returned an invalid status. Performance data returned by counter DLL will not be returned in Perf Data Block. Exception or status code returned is data DWORD 0.

Source: Perflib

ID: 1010

Resolution: A softpaq will be issued to resolve the issue.

AppleTalk Protocol is not supported in a cluster

Services for Macintosh is not supported in cluster configurations since state information is held in local memory and cannot transition between nodes. Using Services for Macintosh in a cluster can result in data loss during cluster failover events. This is detailed in Microsoft Knowledge Base article 243839.

Drive Letters on drive volume letters may be reassigned during quick restore

After quick restore of the NAS b3000 v2, drive letters may be reassigned. Shares will still function against the reassigned drives but the reassignment may be unwanted. To reassign the drive letters to their original assignment, access Disks and Volumes via the Disks tab, right-click the drive in question, select change drive letter, and then edit.

Secure Path

Secure Path Manager allows the setting of features that do not apply

Secure Path Manager contains options that may not be relevant to all storage types. For example, the load balancing selections included in the Secure Path Manager interface are not relevant to storage elements created on the MSA1000 storage subsystem. Even though the Secure Path Manager interface appears to manage load balancing settings for the MSA1000, the settings will not persist because load balancing is not supported with this type of storage.

Cannot retrieve status or manage Secure Path 4.0

When adding hostnames to a profile, the Java applet hangs during the `Gathering agent data, please wait...` phase. No data is gathered and the target host is basically unmanageable from SecurePath. Securepath and the SAN Connection tool erroneously recommend Java2 Runtime 1.3.1 or later, when in fact SecurePath functions correctly only with Version 1.3.1. This version can be installed from *c:\WINNT\bin\SANConnect\SecurePath4Manager\JREs*. Loading newer versions of Java2 Runtime will cause SecurePath Manager to malfunction..

Quick Restore Process

Drive Configuration

The Quick Restore Process is designed to restore the Operating System drives included in the HP StorageWorks NAS system. The two 36GB drives in slots 0 and 1 make up the Operating System drives. If the configuration of the two 36GB drives is altered, then the Quick Restore process may fail to complete properly resulting in the error

```
QuickRestore has detected a hardware failure within your system.
```

The default configuration is:

Array A: Consists of three logical drives and two physical drives in slots 0 and 1

Logical Drive 1:

Raid: 1

Size: 16339MB

Sectors: 32

Stripe Size: 256

Array Accelerator: Enabled

Logical Drive 2:

Raid: 1

Size: 16339MB

Sectors: 32

Stripe Size: 256

Array Accelerator: Enabled

Logical Drive 3:

Raid: 1

Size: 2047MB

Sectors: 32

Stripe Size: 256

Array Accelerator: Enabled

Note: HP recommends that you not change the configuration of Array A.

If the Array and Logical Drive configuration has been altered and the Quick Restore fails to work properly, use the Array Configuration Utility to configure the drives as described above. The Array Configuration Utility is available by booting the system with the SmartStart and support Software CD included with the HP StorageWorks NAS system.



WARNING: Do not replace the Operating System drives with drives that were previously configured on another system. Replace bad drives with **ONLY** blank, unconfigured drives. If necessary, install the drives in another system and use ACU to remove any previous configuration from the drives.

3rd Party Issues

Veritas Backup Exec

Veritas Backup Exec does not back up snapshot directories by default

To back up files using snapshot directories a registry change is required.



WARNING: Using Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. You should backup your Registry before making any changes. Use Registry Editor at your own risk. For information about how to backup, edit, and restore the Registry in Windows 2000, see Microsoft Knowledge Base Article Q322755.

1. Go to a command prompt and run `regedit`.
2. Locate the registry entry:
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup`
3. Remove the entry from the list of files not to backed up which reads Persistent Storage Manager (Images).

Backup of snapshots can now be performed.

Veritas Backup Exec does not restore the files when a snapshot was used for backup by default

To resolve this issue:

1. Select files for restore. Record what the snapshot name is from the set you are restoring
2. Select Redirect to allow the files to be redirected. Select a new directory for restoration. (for example: `e:\hp`)
3. Under the Windows 2000 tab of the restore properties page, locate the Junction Points Control, select the radio button **Preserve Existing Junction Points and restore files and directories from media**.
4. In the directory where you want to do the restore, create the directory with the same name as the snapshot name (`e:\hp\snapshot.1`). The exact directory must be created otherwise Backup Exec will create the directory and make it a junction point that points to the original snapshot. Since the original snapshot is read-only, when it goes to do the restore of a file in it, it will fail with access denied.
5. Begin the restore job.

Alacritech Network Cards

When using the Alacritech Network Cards in conjunction with the NAS b3000 v2, the Alacritech nic can disable Netbios functionality of the embedded HP Network Interface Cards. To resolve the issue, access the device from the local console or the ilo Management Port and uninstall the HP NC7781 network cards and rescan for devices from the device management applet located in the MMC. Rescanning will add back in the embedded nics and allow Netbios to function correctly. HP is working with Alacritech to update their device drivers to resolve the issue.

Blue Screen with "STOP 0x0000007f error when using Terminal Services

Applications that install a kernel driver under the NAS OS such as the Symantec AntiVirus Program may cause the computer to unexpectedly reboot or encounter a blue screen with a STOP message similar to the following:

```
STOP 0x0000007f (0x00000008, 0x00000000, 0x00000000, 0x00000000)
UNEXPECTED_KERNEL_MODE_TRAP
```

NAS devices utilizing a combination of Terminal Services in Remote Administration Mode with a combination of any of the following applications: NAS Data Copy and Columbia Data Product's PSM, Symantec AntiVirus Corporate Edition 8.0, St. Bernard Open File Manager, Quota Manager, Legato RepliStor, or other "filter drivers" that register with the Kernel Stack may exhibit this behavior.

Recommendations to resolve this issue include:

- Disable "Scan floppy disk in A: for boot viruses when shutting down" in the virus scanning program
- Disable "Scan all removable media for boot viruses every time it is mounted" in the virus scanning program
- Uninstall NAS DataCopy if it is not being used
- A registry modification provided by NAV to reduce or limit stack use can be accessed via the link below.

<http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2002071208532048>

Using Norton AntiVirus in conjunction with Terminal Services forces a blue screen

On HP StorageWorks NAS devices, scanning of the floppy drive can result in a blue screen occurrence when logging into the server. To resolve this issue perform, the following steps:

1. Open Norton Anti-Virus.
2. Click Options.
3. In the System section, click Auto-Protect, then click Advanced.
4. In the "What activities to monitor when using floppy disks" section, uncheck "Scan floppy disk in A: for boot viruses when shutting down." and "Scan all removable media for boot viruses every time it is mounted"

The following links provide additional info:

<http://service1.symantec.com/support/ent-security.nsf/d04e6f2f2dfad5de88256c910079502c/b2e1ace5f21a4bf788256c6e0067298f?OpenDocument>

<http://service1.symantec.com/support/ent-security.nsf/d04e6f2f2dfad5de88256c910079502c/085516501e0c91a388256bf4004ac45d?OpenDocument>

Task Scheduler error when creating a policy and running a WQuinn report from version 5.0

When running reports with WQUINN 5.0 the following message appears in the eventlog and the report does not run.

```
"Event Type:Error
Event Source:Schedule
Event Category:None
Event ID:7901
Date: 1/13/2002
Time: 2:00:00 PM
User: N/A
Computer:b3000V2
Description:
The At1.job command failed to start due to the following error:
The system cannot find the file specified.
```

The schedule will list the following program: *C:\Program Files\WQuinn\StorageCentral SRM\5.0\bin\SCReport.exe /F C:\Program Files\WQuinn\StorageCentral SRM\5.0\bin\SR_2002113135833850.txt.*

There is no *SCReport.exe* file located in the *C:\Program Files\WQuinn\StorageCentral SRM\5.0\bin* directory. Hence, the event log error.

Resolution: Upgrade to SRM 5.0 SP1.