



# **Intel<sup>®</sup> Entry Storage System SS4000-E**

## ***Root File System Recovery Script User Guide***

**Document Revision 1.3**

**October 2012**

**Storage Systems Technical Marketing Engineering**

## ***Document Revision History***

<b>Date</b>	<b>Revision Number</b>	<b>Modifications</b>
26 January 2007	1.0	Initial Release
21 February 2007	1.1	Modified section 2.4 - added nas_info information Modified section 2.5 – added nas_user_share_list information Added section 2.6.6 – Configuring Using nas_user_share_list
5 March 2007	1.2	Modified section 2.4.7 – Noted firmware 13.b524 copy and upgrade. Modified section 2.4.7.a – Modified commands to create newpkg subdirectory and copy FW 1.3 pkg file Modified section 2.4.7.b – Added note to indicate script step can take length of time to complete
17 October 2012	1.3	Added prerequisites section 7 to download firmware version 1.3

## ***Disclaimers***

- THIS TRAINING DOCUMENT AND RELATED MATERIALS AND INFORMATION ARE PROVIDED "AS IS" WITH NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY INSTRUCTION, GUIDANCE, PROPOSAL, SPECIFICATION, OR SAMPLE. INTEL ASSUMES NO RESPONSIBILITY FOR ANY ERRORS CONTAINED IN THIS DOCUMENT AND HAS NO LIABILITIES OR OBLIGATIONS FOR ANY DAMAGES ARISING FROM OR IN CONNECTION WITH THE USE OF THIS DOCUMENT.
- This training is not intended for end user marketing for any Intel products featured. Additional product specific disclaimers and legal information may apply. Contact your Intel representative or visit [www.intel.com](http://www.intel.com) for more information.
- Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of Intel products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. Buyers should consult other sources of information to evaluate the performance of systems or components they are considering purchasing.
- Intel Corporation may have patents or pending patent applications, trademarks, copyrights, or other intellectual property rights that relate to the presented subject matter. The furnishing of documents and other materials and information does not provide any license, express or implied, by estoppel or otherwise, to any such patents, trademarks, copyrights, or other intellectual property rights.
- Intel may make changes to this document and related materials, specifications, product descriptions, and plans at any time, without notice.
- INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. INTEL PRODUCTS ARE NOT INTENDED FOR USE IN MEDICAL, LIFE SAVING, OR LIFE SUSTAINING APPLICATIONS.
- \*Other names and brands may be claimed as the property of others.
- Intel and the Intel logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
- Copyright© 2012, Intel Corporation

# Table of Contents

- 1. Introduction.....4
- 2. Loading and Running the Script .....5

# 1. Introduction

---

This User Guide provides instructions on how to restore access to a SS4000-E Entry Storage System using a script that was developed for this process. Manifestations of this loss of access to a user's data are varied and the script will attempt to correct the issue by rebuilding the root file system. .

**CAUTION:** Read these recovery instructions completely.

An error in your implementation may cause your data to be permanently unrecoverable.

The recovery requires SS4000-E Entry Storage System Linux operating system root level command line access. If you are unfamiliar with Linux command line use, Intel recommends that you not attempt to use this recovery software. A command error at root level access can cause unrecoverable damage to the file system.

Intel recommend that the utility being used as the console interface, HyperTerminal, ProComm Plus, other, be setup to capture the output of the script.

Your data may not be accessible even after running this recovery script. This software is provided royalty free "AS IS" with no warranty whatsoever, including any warranty of merchantability, fitness for any particular purpose, or any warranty otherwise arising out of any proposal, specification, or sample, strictly for the convenience of Intel customers. Customers use this script at their own risk. Intel will provide no support for script use. Intel provides no guarantee that executing the script will result in data recovery.

## 2. Loading and Running the Script

---

### 2.1 Applicable Firmware Versions

This script will reconstruct the root file system and recover NAS data for v1.0, v1.1, v1.2 and v1.3 of the firmware if possible. It is possible that manual intervention may be required after running the script. After the script is run and has completed, the user will have to rebuild the configuration. The recovery process will, by using firmware 1.3 Build 524 called out in the procedure below, update versions v1.0, v1.1 and v1.2 to v1.3. An SS4000-E Entry Storage System already at v1.3 firmware will be rebuilt using the v1.3 firmware.

### 2.2 Limitations

The v1.1 Korean firmware is not supported by this script. If a case of a customer losing access to their data is reported that is running the Korean v1.1 firmware, it will require manual restoration.

### 2.3 Prerequisites

It is preferred to use a serial console connection rather than a SSH / Telnet session. The following process can be followed.

1. A system with a serial port connection and two Ethernet network ports
2. Acquire a DH-10 to DB-9 serial cable.
3. Remove SS4000 cover, and attach the DH10 connector to the SS4000 (behind the memory DIMM socket toward the back of the board).
4. Configure HyperTerminal or a console communication application such as ProComm Plus can be used.
  - A. Use appropriate COM port
  - B. 115K bits per second, 8 Data bits, No Parity, 1 Stop bit and No Hardware flow control
5. Determine IP address you will be using for TCP/IP session
  - A. Press Enter to get a login prompt. It may take up to 30 seconds for the prompt to appear
  - B. Log in as root/storage
  - C. If this is successful, go to step D below. If this login is unsuccessful, then
    - A. Use the reset button on the back of the system to reset the administrator username, password and network IP address to the default values. This can be found on the back of the system next to Ethernet Port 1. The following symbol is shown above the location: "/". The button is recessed and you can use a pen to reset the machine's password and network configuration. Press this button for 5 seconds and release
    - B. Log in as root/storage
    - C. If this login is unsuccessful, then
      - i. Power down the system
      - ii. Unplug all HDDs
      - iii. Power on the system, and then login again.
      - iv. If this is successful, hot plug all HDDs

- D. Run "ifconfig" from the # prompt
- E. Note the IP address and subnet mask of the unit
- 6. Configure one Ethernet port to connect to the SS4000 system and direct connect the two systems.
  - A. A TFTP server should be available to accommodate loading the script.
  - B. An established network connection between the TFTP server and the SS4000 unit
  - C. A TFTP server agent may be required for the system connected to the SS4000. TFTP32 is such an agent and can be found at <http://tftpd32.jounin.net/> or <http://www.tftp-server.com/>. No installation should be required after download.
  - D. Start the tftp agent (double click on the filename in Windows Explorer or other method).
  - E. Set the base directory to the directory containing the extracted files Re-init.sh & nas\_info (extract the files using WinZip).
- 7. Firmware 1.3 Build 524 available for transfer to the SS4000-E as part of the recovery process (Procedure section 7a below). Firmware 1.3 Build 524 can be downloaded from <http://downloadcenter.intel.com/> by searching for SS4000-E in the search box. Systems with firmware revisions below 1.3 will be updated to 1.3 through the recovery procedure.
  - A. **Note:** Firmware revision 1.4 is not supported by this recovery script because the capacity in the storage system is divided into multiple partitions which is not supported for recovery. **Overwriting a 1.4 firmware system with firmware 1.3 Build 524 is data destructive.**

## 2.4 Procedure

This section describes the steps required to run the script. It is very lengthy and quite involved. Please read each step carefully and ensure you are executing each correctly.

1. Power off the SS4000-E system and pull all the disks out of the connectors – the disks do not have to be removed from the chassis, only disconnected from the connectors on the backplane.
2. Power on the SS4000-E system.
  - a. Wait 2 – 3 minutes to ensure the system has booted into what is called "RAM mode". Part of the boot sequence is generating a secret key for SSH (specifically in v1.1 and v1.2 of the firmware) and requires some time to complete this process. If the system booted into RAM mode successfully the system status LED should be solid amber.
3. Plug in the disks into the SS4000-E one at a time. Wait for each LED on the disk drive carrier to light up (LED should be solid green).
4. If you could not use a serial console setup then use the SSC (Storage System Console) to discover the SS4000-E system.
  - a. Login to the system using the default IP address (192.168.0.101 on port 1).

- b. For v1.0 you can telnet directly to the system using the IP address. For v1.1 and v1.2 you must first enable SSH. Now that the login has been established, enter the following URL into the address bar of your browser:
  - c. [https://192.168.0.101/ssh\\_controlF.cgi](https://192.168.0.101/ssh_controlF.cgi)
  - d. This should open a page that has the option of enabling SSH. Turn on SSH.
  - e. Login via telnet or SSH (this will require running a utility such as PuTTY on Windows) using the default username: root and default password: storage.
5. If you have a serial console session established you should be able to press “Enter” and get a login prompt. Enter the default username: root and default password: storage to login.
6. Once logged into the system you must ensure all disks are recognized in the Linux system before running the script. As an example:
  - a. Enter the following command at the prompt:

```
# cat /proc/scsi/scsi
```

This is an example of the output from the command. Your output may differ depending on you disk number or manufacturer and models installed. Here four disks are installed.

Attached devices:

```
Host: scsi0 Channel: 00 Id: 00 Lun: 00
Vendor: Unknown Model: ST3750640AS Rev: 3.AA
Type: Direct-Access ANSI SCSI revision: 02
Host: scsi0 Channel: 01 Id: 00 Lun: 00
Vendor: Unknown Model: ST3750640AS Rev: 3.AA
Type: Direct-Access ANSI SCSI revision: 02
Host: scsi0 Channel: 03 Id: 00 Lun: 00
Vendor: Unknown Model: ST3750640AS Rev: 3.AA
Type: Direct-Access ANSI SCSI revision: 02
```

7. You now will transfer the script and the 1.3 firmware package to the SS4000-E system by reading it from the TFTP server. During the system recovery the script will install firmware version 1.3 from the newpkg subdirectory. Enter the following commands:
  - a. Enter the following commands on the SS4000-E

```
# cd /tmp
# mkdir newpkg
# cd newpkg
# tftp -g <IP address of the TFTP server> -r fs-bc-1.3-b524.pkg
# cd ..
# tftp -g <IP address of the TFTP server> -r Re-init.sh
# tftp -g <IP address of the TFTP server> -r nas_info
# chmod +x Re-init.sh nas_info
```

- b. Execute the Re-init.sh script by executing the following command:  

```
# /tmp/Re-init.sh
```
8. If the script runs properly without errors, it displays “RESULT is 1”. Otherwise, is there is an error it displays “Abort!!” or “RESULT is 0”.
  - a. **Note:** The following script command can take 5 to 10 minutes to complete:  

```
/fs/writeflash -p /newpkg/fs.pkg
```

The script will pause and appear to hang until this completes. Do not restart or power cycle system. Wait for a Result code.
9. Reboot the SS4000-E system using the following command via the serial console:

```
# sync;sync;reboot
```

The system should boot up successfully with a clean configuration. You can browse the Users / Groups/ Shared Folders pages in the web management console UI and they should appear the same as they did after the first initialization operation.

There are 5 files saved in the /nas/NASDisk-00002/public directory or folder during the recovery process that can be used for manual configuration. The next item will discuss manual configuration to rebuild the configuration in the web console UI.

## 2.5 Saved Configuration Files

After the script runs completely, the system should be able to boot up from a clean root file system and the NAS should function correctly. Once the system is booted ssh (v1.1 and v1.2) or telnet (v1.0) into the system and go to /nas/NASDisk-00002/public/bcbox.recover.\${timestamp}. There are 6 text files saved:

1. userlist
2. sharelist
3. unas.conf
4. nasuser.conf
5. nas.conf
6. nas\_user\_share\_list

The function of each is described below.

- **userlist:** This file keeps names of all home folders. For every CIFS user in local mode, there should be a home folder with the same name as the user account name when the user account was created. The home folders are stored in the user RAID, not in the root file system. This file can be referred to when you want to create CIFS users in the local mode.
- **sharelist:** This file keeps names for all the shared folders except usbdisk1, usbdisk2 and home folders. The shared folders are stored in the user RAID not the root file system. This file can be referred to when you want to create shared folders.
- **unas.conf:** This file keeps the system configurations, like hostname, configured IP, etc. This file is stored in the root file system and may be damaged due to root file



system corruption. This file can be referred to when you want to set the system configurations.

- **nasuser.conf:** This file keeps the CIFS user and group accounts. This file is stored in the root file system and may be damaged due to root file system corruption. The CIFS users listed in this file should be the same as those listed in 'userlist'. This file should be referred to first and if it is corrupted, userlist is referred to instead.
- **nas.conf:** This file keeps the shared folder assignment and NFS user list. This file is stored in the root file system and may be damaged due to root file system corruption. This file can be referred to when you want to create NFS users and assign shared folders to CIFS/NFS users.
- **Nas\_user\_share\_list:** This file contains the data parsed by nas\_info from nasuser.conf and nas.conf. Due to the complexity of nas.conf and nasuser.conf, this file lists the CIFS/NFS user/group/assignments which helps the configuration rebuild process.

## 2.6 Steps to Rebuild the Configurations

To rebuild the configurations, please follow the process in the Web GUI.

**NOTE:** if the system is set to Active Directory mode in v1.2, the shared folder assignments can not be completed due to lack of the required Active Directory server. To assign a shared folder to a user, the user must be seen by the storage system. If the mode is Active Directory mode, the system is not able to sync the Active Directory users into the system because the Active Directory information is in the end user's environment. This prevents the shared folder assignments from configuring. To resolve this, the end user would have to assign the shared folder themselves when they receive the restored system. In this case, only steps 1, 2 and 4 can be done. To look up what authentication mode the system uses, please review section 2.6.5.

1. Enable SSH manually in v1.1 and v1.2. This is to look up the files stored in `/nas/NASDisk-00002/public/bcbox.recover.${timestamp}` and `/usr/local/ipstor/etc/${hostname}/`.
2. Based on data from `unas.conf`, configure the system.
3. If a `nas_user_share_list` file is present do the following:
  - a. Based on data from the `nas_user_share_list` file, create CIFS users and groups. This will also rebuild the relationship between the user account and its home folder. Create shared folders except the public, `usbdisk1` and `usbdisk2` shared folders. Create NFS users and assign the shared folders to users / groups.
4. If no `nas_user_share_list` file is present do the following:
  - a. Based on data from `nasuser.conf` and `userlist`, create CIFS users and groups. This will also rebuild the relationship between the user account and its home folder.
5. Based on data from `sharelist`, create shared folders except public, `usbdisk1` and `usbdisk2`.
6. Based on data from `nas.conf`, create NFS users and assign the shared folders to users/groups.

The following examples give more details on the above steps. (check `/nas/NASDisk-00002/public/bcbox.recover.${timestamp}`).

### 2.6.1 Configuring Using unas.conf

Text following "<==" are comments. There are some fields not listed in this example because they are not changeable in the Web GUI, except the admin password which cannot be displayed as it is encrypted.

```

HOSTNAME="EM7210qaqa"           <== Hostname of this storage system.
    There is no need to change the hostname in the Web GUI because the script
    already sets the hostname to the value kept in this file.
WORKGROUP="WorkGroup"          <== Workgroup name
TIMEZONE="GMT-8"                <== Time zone
ADMIN_NAME_0="admin"            <== Admin account name
DHCP_0="1"                      <== Port 1, DHCP client function is
    enabled(1) or disabled(0)
IP_0="192.168.0.101"            <== Port 1, if DHCP client is disabled, this
    is the "IP address"
NETMASK_0="255.255.255.0"       <== Port 1, if DHCP client is disabled, this
    is the "Subnet mask"
GATEWAY_0="0.0.0.0"             <== Port 1, if DHCP client is disabled, this
    is the "Gateway IP address"
DNS_0="0.0.0.0"                 <== Port 1, if DHCP client is disabled, this
    is the "Preferred DNS server"
DNS_1="0.0.0.0"                 <== Port 1, if DHCP client is disabled, this
    is the "Alternate DNS server"
DHCP_0="0"                      <== Port 1, if DHCP client is disabled,
    enable (1) or disable (0) DHCP server
DHCP_0_START="192.168.0.102"     <== Port 1, if DHCP client is disabled and
    DHCP server is enabled, This is the "Starting IP address"
DHCP_0_END="192.168.0.254"       <== Port 1, if DHCP client is disabled and
    DHCP server is enabled, this is the "Ending IP address"
FTPS="0"                        <== FTP server is enabled(1) or
    disabled(0)
DHCP_1="1"                      <== Port 2, DHCP enable(1) or disable(0)
IP_1="192.168.1.101"            <== Port 2, if DHCP is disabled, this is the
    "IP address"
NETMASK_1="255.255.255.0"       <== Port 2, if DHCP is disabled, this is the
    "Subnet mask"
NTP=""                          <== NTP server name or its IP
    address
MTU_0="1500"                    <== Port 1, MTU size (Jumbo Frame size -
    14 bytes (MAC frame header))
MTU_1="1500"                    <== Port 2, MTU size (Jumbo Frame size -
    14 bytes (MAC frame header))

```

### 2.6.2 Configuring Using nasuser.conf

The nasuser.conf is used to create the CIFS users and groups and rebuild the relationship between the user account and its home folder. Some descriptive header lines are removed for ease of reading.

```

<WindowsClientList userSyncInterval="0" windowsServerID="">
<WindowsUserList nextUserID="6">
<WindowsUser userID="2" systemUID="64436" unixUserName="guest"
  windowsName="guest" comment="Local User" windowsUID="0"/>
<WindowsUser userID="3" systemUID="64437" unixUserName="cifsu1"
  windowsName="cifsu1" comment="Local User" windowsUID="0"/>
<WindowsUser userID="4" systemUID="64438" unixUserName="cifsu2"
  windowsName="cifsu2" comment="Local User" windowsUID="0"/>
<WindowsUser userID="5" systemUID="64439" unixUserName="cifsu3"
  windowsName="cifsu3" comment="Local User" windowsUID="0"/>
</WindowsUserList>
<WindowsGroupList nextGroupID="3">
<WindowsGroup groupID="1" systemGID="75" unixGroupName="group1"
  windowsName="group1" comment="Nas Group" windowsGID="0">
<WindowsGroupMemberList>
<WindowsGroupMember userID="4"/>
<WindowsGroupMember userID="5"/>
</WindowsGroupMemberList>
</WindowsGroup>
<WindowsGroup groupID="2" systemGID="76" unixGroupName="group2"
  windowsName="group2" comment="Nas Group" windowsGID="0">
<WindowsGroupMemberList>
<WindowsGroupMember userID="3"/>
<WindowsGroupMember userID="5"/>
</WindowsGroupMemberList>
</WindowsGroup>
</WindowsGroupList>
</WindowsClientList>

```

Use `WindowsUser` as a keyword to look for available CIFS users. In this example, there are 4 users:

```

User "guest", the uid is 64436, and the userID is 2
User "cifsu1", the uid is 64437, and the userID is 3
User "cifsu2", the uid is 64438, and the userID is 4
User "cifsu3", the uid is 64439, and the userID is 5

```

Create 4 CIFS users in the Web GUI. For every user created, the storage system will keep its info in `/usr/local/ipstor/etc/$(hostname)/nasuser.conf`. `$(hostname)` represents the hostname of the storage system. For simplicity, name `/nas/NASDisk-00002/public/bcbox.recover.$(timestamp)/nasuser.conf` as `old_nasuser.conf`, and name `/usr/local/ipstor/etc/$(hostname)/nasuser.conf` as `new_nasuser.conf`. Compare the created user's uid listed in `oldnasuser.conf` and `new_nasuser.conf`. If they are the same, the user's home folder is now accessible. If they are not the same, please change the owner of the home folder to the user. The home folders for all users are under `/nas/NASDisk-0002/homes` directory.

For instance, `cifsu1`'s uid in the `old_nasuser.conf` is 64437, if the uid located in `new_nasuser.conf` is not the same value, change the owner of the home folder to the user.

```
#chown -R cifsu1 /nas/NASDisk-00002/homes/cifsu1
```

Use WindowsGroup as a keyword to look for available CIFS groups. In this example, there are 2 groups:

In this example, there are 4 users.

group "group1", the gid is 75, the groupID is 1 and this group contains two users  
cifsu2 (userID 4) and cifsu3 (userID 5)

group "group2", the gid is 76, the groupID is 2 and this group contains two users  
cifsu1 (userID 3) and cifsu3 (userID 5)

Create 2 groups in the Web GUI and add the users into each group. For each created group, the storage system will keep its info in /usr/local/ipstor/etc/\$(hostname)/nasuser.conf.

### 2.6.3 Configuring Using userlist When nasuser.conf Is Damaged Or Lost

If the nasuser.conf file is damaged or lost userlist is used for configuration. Type the following command at the command prompt.

```
#cat /nas/NASDisk-00002/public/bcbox.recover.1169104833/userlist
```

An example output:

```
cifsu1
cifsu2
cifsu3
```

The number 1169104833 is a time stamp generated when the script runs. There are 3 home folders and this means there should be 3 CIFS users in local mode. Create these users in the Web GUI. To check if the user's home folder is accessible, follow these steps:

1. list the home folders by `ls -al` and look for the line containing the home folder you want to check.

```
# ls -al
drwxrwx--- 5 root    nasgrp    62 Jan 18 06:59 .
drwxrwx--- 8 root    nasgrp    132 Jan 18 07:03 ..
drwxr-x--- 2 cifsu1  nasgrp     8 Jan 18 06:58 cifsu1
drwxr-x--- 2 64438  nasgrp     8 Jan 18 06:59 cifsu2
drwxr-x--- 2 64439  nasgrp     8 Jan 18 06:59 cifsu3
```

2. Get the uid/username of the home folder. The 3rd column is the uid/username of the home folder's owner. If you create the CIFS user from web GUI, the system is able to associate the username and his/her uid. The 3rd column will then display the username, not uid. The 3rd column displays uid when the storage system can not associate a username with a uid. Line 3 is an example (cifsu1) where the system is able to associate the username and its uid.
3. If the home folder's name equals the owner's username (like line 3), the home folder should be accessible by the owner. Otherwise, if the 3rd column is a uid, please look

up the uid kept in /usr/local/ipstor/etc/\$(hostname)/nasuser.conf by using the home folder name. If both uids are the same, the home folder should be accessible by the owner. Otherwise, you must change the owner of the home folder to the owner whose username is the same as the home folder by a command such as the following:

```
#chown -R cifsu1 /nas/NASDisk-00002/homes/cifsu1
```

## 2.6.4 Configuring Using sharelist

At the command prompt enter the following command:

```
#cat /nas/NASDisk-00002/public/bcbox.recover.1169104833/sharelist
```

Sample output:

```
public
share1
```

The number 1169104833 is a time stamp generated when the script runs. There is 1 shared folder and you have to create it in the Web GUI. This will not affect the data in that shared folder. Rather, this enables the root file system to keep track of this shared folder "share1".

## 2.6.5 Configuring Using nas.conf

To create the NFS users and shared folder assignments you can use the information in the nas.conf file. Only the relevant parts of the configuration file required for configuration reconstruction are shown here and explained.

1. Authentication mode type of the system.  

```
<WindowsProperties workgroup="WorkGroup" netBiosName="EM7210qaqa"
security="USER" securitySubType="None"
~~~~~
passwordServer="" comment="Storage System" clientCodePage="437"
codingSystem=""
codePageLibPath="/usr/local/ipstor/lib/codepages" bindInterfaceOnly="false"
auditEnabled="false">
```

The tag above the symbol ~ has two values: "USER" or "ADS". "USER" means the mode is local authentication mode, "ADS" means the mode is AD mode.

2. Parent directory of the user's home folder. Find keyword SMBHomes to identify the start of this section  

```
<NASShare shareID="0" vdevID="0" path="/nas/NASDisk-00002/homes">
~~~~~
```

The tag above the symbol ~ indicates the parent directory of the user's home folder. For instance, the user guest's home folder path would be /nas/NASDisk-00002/homes/guest.

3. NFS users. Find the keyword NFSCientList to identify the start of this section.  

```
<NFSCientList nextClientID="3" squashGID="11578">
  <NFSCient id="1" label="nfsu1" machine="172.31.32.1" comment=""/>
  <NFSCient id="2" label="nfsu2" machine="172.30.0.0/16" comment=""/>
```

```
~~~~~
</NFSCClientList>
```

Above the ~, there are two NFS users found. The following are the details of each NFS user. The computer description is "nfsu1", the IP address or computer name is "172.31.32.1", and the NFS client id "1". The second computer description is "nfsu2", the IP address or computer name is "172.30.0.0/16", and the NFS client id "2". From the above info, you should be able to create the NFS users.

4. Share folder assignment (For user/group reconstruction, please refer to section 2.6.3 about nasuser.conf). Find NASShareList to identify the start of this section. From the following information, you should be able to determine which folder is assigned to which CIFS users/groups and NFS users and create the assignment in the Web GUI.

Example 1:

```
<NASShare shareID="5" vdevID="2" path="/nas/NASDisk-00002/share1">
<WindowsShare shareName="share1" maxConnect="0" comment="" available="true"
audit="false" auditPath="" vfsObject="" vfsOptions="">
```

~~~~~  
The share folder is named "share1".

```
<GroupAssignmentList>
<GroupAssigned id="2" access="ReadWrite"/>
```

~~~~~  
This shared folder is assigned to 1 group. Group name group2 (group id 2) with Read/Write permission. You have to look up the group name with group 2 in the nasuser.conf file.

```
</GroupAssignmentList>
```

```
<UserAssignmentList>
<UserAssigned id="3" access="ReadWrite"/>
<UserAssigned id="4" access="ReadWrite"/>
```

~~~~~  
This shared folder is assigned to two users. User name cifsu1 (user id 3) has Read/Write permission. You have to look up the CIFS username with user id 3 in the nasuser.conf file. User name cifsu2 (user id 4) has Read/Write permission. You have to look up CIFS username with user id 4 in the nasuser.conf file.

```
</UserAssignmentList>
<VFSObjects/>
<Infoltem name="nt acl support" value="no"/>
</WindowsShare>
```

```
<NFSCClientAssignmentList>
<NFSCClientAssignment id="1" squash="no" secure="true" access="ReadWrite"
nfs_sync="false" no_wdelay="false"/>
```

```

~~~~~
~~~~~
User name nfsu1 (NFS client id 1) has ReadWrite permission. You have to look up
the NFS username with NFS client id 1 in the nas.conf file.

</NFSClientAssignmentList>
</NASShare>

```

## 2.6.6 Configuring Using nas\_user\_share\_list

The nas\_user\_share\_list file can be user to create the NFS users, CIFS users/groups and shared folder assignments.

To generate nas\_user\_share\_list again, follow the steps below.

1. A requirement is the ipstor library exists. To confirm the ipstor library exists do the following.
2. Logged onto the system via the terminal session or SSH, at the prompt type:
 

```
# ls .is.sh
```

 or type:
 

```
# ls -la | more
```

 (the output of this command is a listing of the directory and somewhere close to the beginning of the listing you should see .is.sh)
3. Run nas\_info
 

```
usage: nas_info <nas.conf> <nasuser.conf>
```

  - a. To execute nas\_info use the following commands:
  - b. 

```
# cd /
```
  - c. 

```
# ./etc/.is.sh
```
  - d.

Execution:

- a. 

```
# ./etc/.is.sh
```
- b. 

```
# cd /tmp
```
- c. 

```
# ./tmp/nas_info /usr/local/ipstor/etc/`Host_Name`/nas.conf
    /usr/local/ipstor/etc/`Host_Name`/nasuser.conf > nas_user_share_list
```

As an example you can review the following:

```
# nas_info /usr/local/ipstor/etc/EM7210/nas.conf
/usr/local/ipstor/etc/EM7210/nasuser.conf
```

```
==> cifs user guest, uid 64436
```

```
~~~~~
```

```
CIFS user "guest", uid 64436
```

```
==> cifs user user1, uid 64437
```

```
==> cifs user user2, uid 64438
```

```
==> cifs user user3, uid 64439
```

```
==> cifs group group1, gid 11582 >>> member user1, user3
```

```
~~~~~
```

```
CIFS group "group1", gid 11582, has two members: user1 and user3
```

```
==> cifs group group2, gid 11583 >>> member guest, user2
```

```
==> nfs computer description nfs1, ip address or computer name 172.31.32.1
```

```
~~~~~
```

```
NFS computer description "nfs1", IP address or computer name: 172.31.32.1
```

```
==> nfs computer description nfs2, ip address or computer name 172.30.1.1
```

```
==> nfs computer description nfs3, ip address or computer name 172.31.0.0/16
```

```
=====
```

```
==> share name: public
```

```
~~~~~
```

```
Share folder name "public"
```

```
--> cifs user guest, permission ReadWrite
```

```
~~~~~
```

```
Public share folder is assigned to CIFS user "guest" with read/write permission
```



--> cifs user user1, permission ReadWrite

--> cifs user user2, permission ReadWrite

--> cifs user user3, permission ReadWrite

--> nfs name nfs1, permission ReadWrite

~~~~~

Public share folder is assigned to NFS user "nfs1" with read/write permission

--> nfs name nfs2, permission ReadWrite

--> nfs name nfs3, permission ReadWrite

==> share name: usbdisk1

~~~~~

usbdisk1 share folder has no assignment

==> share name: usbdisk2

==> share name: share1

--> cifs user guest, permission ReadOnly

~~~~~

share1 share folder is assigned to CIFS user "guest" with read only permission

--> cifs user user1, permission ReadWrite

--> nfs name nfs1, permission ReadWrite

--> nfs name nfs3, permission ReadOnly

--> cifs group group2, permission ReadOnly

==> share name: share2

--> cifs user user1, permission ReadOnly

```
--> cifs user user3, permission ReadWrite
```

```
--> nfs name nfs2, permission ReadOnly
```

```
--> cifs group group2, permission ReadWrite
```

```
~~~~~
```

share2 share folder is assigned to CIFS group "group1", "group2" with read/write permission