## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>10</td>
</tr>
<tr>
<td>Document Revision Level</td>
<td>10</td>
</tr>
<tr>
<td>Contacting Hitachi Data Systems</td>
<td>10</td>
</tr>
<tr>
<td>Related Documentation</td>
<td>10</td>
</tr>
<tr>
<td>1 File system formats</td>
<td>14</td>
</tr>
<tr>
<td>File system access protocols</td>
<td>16</td>
</tr>
<tr>
<td>File system tiers</td>
<td>16</td>
</tr>
<tr>
<td>Tiered file systems and snapshots</td>
<td>17</td>
</tr>
<tr>
<td>Creating a normal file system</td>
<td>18</td>
</tr>
<tr>
<td>Read caches</td>
<td>21</td>
</tr>
<tr>
<td>WORM file systems</td>
<td>22</td>
</tr>
<tr>
<td>WORM file system characteristics</td>
<td>22</td>
</tr>
<tr>
<td>Deduplication file systems</td>
<td>23</td>
</tr>
<tr>
<td>Deduplication characteristics</td>
<td>23</td>
</tr>
<tr>
<td>Deduplication interoperability with existing Hitachi NAS Platform features</td>
<td>23</td>
</tr>
<tr>
<td>Calculating Dedupe space savings</td>
<td>24</td>
</tr>
<tr>
<td>Viewing deduped file system usage</td>
<td>25</td>
</tr>
<tr>
<td>Cloning files</td>
<td>26</td>
</tr>
<tr>
<td>File clone commands</td>
<td>27</td>
</tr>
<tr>
<td>Tree clone commands</td>
<td>27</td>
</tr>
<tr>
<td>2 Managing file system performance</td>
<td>30</td>
</tr>
<tr>
<td>Using the per-file system throttle feature</td>
<td>31</td>
</tr>
<tr>
<td>Creating a read cache file system</td>
<td>31</td>
</tr>
<tr>
<td>Viewing available file systems</td>
<td>35</td>
</tr>
<tr>
<td>Displaying file system details</td>
<td>37</td>
</tr>
<tr>
<td>Formatting a file system</td>
<td>41</td>
</tr>
<tr>
<td>Mounting a file system</td>
<td>42</td>
</tr>
<tr>
<td>Unmounting a file system</td>
<td>42</td>
</tr>
<tr>
<td>Deleting a file system</td>
<td>43</td>
</tr>
</tbody>
</table>
Configuring CIFS security..........................................................................................137
Assigning CIFS names............................................................................................138
Viewing CIFS Setup...............................................................................................138
Joining an Active Directory.....................................................................................141
Removing CIFS sever names..................................................................................144
Configuring local groups.......................................................................................144
    - Adding a local group or local group members.................................................145
    - Deleting a local group or local group members..............................................147
Configuring CIFS shares.......................................................................................147
    - Adding CIFS share..........................................................................................147
    - Displaying and modifying CIFS shares details.................................................153
    - Controlling access to shares using qualifiers..................................................156
    - Controlling access to shares using permissions..............................................157
    - Adding or changing CIFS share access permissions........................................158
    - Offline file access modes.............................................................................159
    - Backing up and restoring CIFS shares............................................................159
Using Windows server management........................................................................160
    - Using the computer management tool...........................................................161
Restoring a previous version of a file......................................................................161

6 Transferring files with FTP..............................................................................162
    - FTP protocol support.......................................................................................163
    - Configuring FTP preferences..........................................................................163
    - Displaying FTP users......................................................................................165
    - Adding an FTP user........................................................................................167
    - Importing an FTP user...................................................................................168
    - Modifying FTP users......................................................................................169
    - FTP statistics..................................................................................................170
    - Configuring FTP audit logging......................................................................170

7 Block-level access through iSCSI....................................................................172
    - iSCSI support..................................................................................................173
    - iSCSI MPIO......................................................................................................174
    - iSCSI access statistics....................................................................................175
    - iSCSI prerequisites.........................................................................................175
    - Supported iSCSI initiators..............................................................................175
    - Offload engines..............................................................................................175
Configuring iSCSI.................................................................................................175
    - Configuring iSNS...........................................................................................176
    - Viewing iSNS servers.....................................................................................176
Configuring iSCSI Logical Units..........................................................................177
    - Logical unit management.................................................................................177
    - Logical unit security........................................................................................178
    - Concurrent access to logical units....................................................................178
    - Taking snapshots of logical units.....................................................................178
    - Volume full conditions....................................................................................179
Managing iSCSI logical units...............................................................................179
    - Viewing the properties of iSCSI Logical Units...............................................180
    - Adding iSCSI logical units..............................................................................182
    - Modifying an iSCSI logical unit......................................................................184
Deleting an iSCSI logical unit................................................................. 185
Backing up iSCSI logical units............................................................... 185
Restoring iSCSI logical units............................................................... 186
Setting up iSCSI targets...................................................................... 186
Viewing the properties of iSCSI targets.............................................. 187
Adding iSCSI targets......................................................................... 188
Adding a logical unit to an iSCSI target............................................... 191
Modifying the properties of an iSCSI Target........................................ 192
Deleting an iSCSI target..................................................................... 194
Configuring iSCSI security (mutual authentication)............................ 194
Configuring the storage server for mutual authentication.................... 194
Changing the storage server's mutual authentication configuration .... 196
Configuring the Microsoft iSCSI initiator for mutual authentication..... 197
Accessing iSCSI storage ..................................................................... 198
Using iSNS to find iSCSI targets.......................................................... 199
Using target portals to find iSCSI targets............................................ 199
Accessing available iSCSI targets....................................................... 200
Verifying an active connection............................................................ 201
Terminating an active connection....................................................... 201
Using Computer Manager to configure iSCSI storage......................... 201

8 Using Hitachi Dynamic Provisioning.................................................. 204
HDP high-level process........................................................................ 205
Understanding HDP thin provisioning................................................ 205
Understanding how HDP works with HNAS....................................... 206
In PDF format, this guide explains about file system formats, and provides information about creating and managing file systems, and enabling and configuring file services (file service protocols).

### Document Revision Level

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MK-92HNAS006-00</td>
<td>August 2012</td>
<td>First publication</td>
</tr>
<tr>
<td>MK-92HNAS006-01</td>
<td>June 2013</td>
<td>Revision 1, replaces and supersedes MK-92HNAS006-00.</td>
</tr>
<tr>
<td>MK-92HNAS006-02</td>
<td>November 2014</td>
<td>Revision 2, replaces and supersedes MK-92HNAS006-01.</td>
</tr>
<tr>
<td>MK-92HNAS006-04</td>
<td>September 2014</td>
<td>Revision 4, replaces and supersedes MK-92HNAS006-03.</td>
</tr>
</tbody>
</table>

### Contacting Hitachi Data Systems

2845 Lafayette Street  
Santa Clara, California 95050-2627  
U.S.A.  
https://portal.hds.com  
North America: 1-800-446-0744

### Related Documentation

**Release Notes** provide the most up-to-date information about the system, including new feature summaries, upgrade instructions, and fixed and known defects.

**Administration Guides**

- **System Access Guide** (MK-92HNAS014)—In PDF format, this guide explains how to log in to the system, provides information about accessing the NAS server/cluster CLI and the SMU CLI, and provides information about the documentation, help, and search capabilities available in the system.
• **Server and Cluster Administration Guide** (MK-92HNAS010)—In PDF format, this guide provides information about administering servers, clusters, and server farms. Includes information about licensing, name spaces, upgrading firmware, monitoring servers and clusters, the backing up and restoring configurations.

• **Storage System User Administration Guide** (MK-92HNAS013)—In PDF format, this guide explains user management, including the different types of system administrator, their roles, and how to create and manage these users.

• **Network Administration Guide** (MK-92HNAS008)—In PDF format, this guide provides information about the server's network usage, and explains how to configure network interfaces, IP addressing, name and directory services.

• **File Services Administration Guide** (MK-92HNAS006)—In PDF format, this guide explains about file system formats, and provides information about creating and managing file systems, and enabling and configuring file services (file service protocols).

• **Data Migrator Administration Guide** (MK-92HNAS005) —In PDF format, this guide provides information about the Data Migrator feature, including how to set up migration policies and schedules.

• **Storage Subsystem Administration Guide** (MK-92HNAS012)—In PDF format, this guide provides information about managing the supported storage subsystems (RAID arrays) attached to the server/cluster. Includes information about tiered storage, storage pools, system drives (SDs), SD groups, and other storage device related configuration and management features and functions.

• **Snapshot Administration Guide** (MK-92HNAS011)—In PDF format, this guide provides information about configuring the server to take and manage snapshots.

• **Replication and Disaster Recovery Administration Guide** (MK-92HNAS009) —In PDF format, this guide provides information about replicating data using file-based replication and object-based replication, provides information on setting up replication policies and schedules, and using replication features for disaster recovery purposes.

• **Antivirus Administration Guide** (MK-92HNAS004)—In PDF format, this guide describes the supported antivirus engines, provides information about how to enable them, and how to configure the system to use them.

• **Backup Administration Guide** (MK-92HNAS007)—In PDF format, this guide provides information about configuring the server to work with NDMP, and making and managing NDMP backups. Also includes information about Hitachi NAS Synchronous Image Backup.

• **Command Line Reference**—Opens in a browser, and describes the commands used to administer the system.

---

**Note:** For a complete list of Hitachi NAS open source software copyrights and licenses, see the System Access Guide.
Hardware References

- *Hitachi NAS Platform 3080 and 3090 G1 Hardware Reference (MK-92HNAS016)*—Provides an overview of the second-generation server hardware, describes how to resolve any problems, and replace potentially faulty parts.
- *Hitachi NAS Platform 3080 and 3090 G2 Hardware Reference (MK-92HNAS017)*—Provides an overview of the second-generation server hardware, describes how to resolve any problems, and replace potentially faulty parts.
- *Hitachi NAS Platform Series 4000 Hardware Reference (MK-92HNAS030)* (MK-92HNAS030)—Provides an overview of the Hitachi NAS Platform Series 4000 server hardware, describes how to resolve any problems, and how to replace potentially faulty components.
- *Hitachi High-performance NAS Platform (MK-99BA012-13)*—Provides an overview of the NAS Platform 3100/NAS Platform 3200 server hardware, and describes how to resolve any problems, and replace potentially faulty parts.

Best Practices

- *Hitachi USP-V/VSP Best Practice Guide for HNAS Solutions (MK-92HNAS025)*—The HNAS practices outlined in this document describe how to configure the HNAS system to achieve the best results.
- *Hitachi Unified Storage VM Best Practices Guide for HNAS Solutions (MK-92HNAS026)*—The HNAS system is capable of heavily driving a storage array and disks. The HNAS practices outlined in this document describe how to configure the HNAS system to achieve the best results.
- *Hitachi NAS Platform Deduplication Best Practice (MK-92HNAS031)*—This document provides best practices and guidelines for using HNAS Deduplication.
- *Hitachi NAS Platform Data Migrator to Cloud Best Practices Guide (MK-92HNAS045)*—Data Migrator to Cloud allows files hosted on the HNAS server to be transparently migrated to cloud storage, providing the benefits associated with both local and cloud storage.
- *Brocade VDX 6730 Switch Configuration for use in an HNAS Cluster Configuration Guide (MK-92HNAS046)*—This document describes how to configure a Brocade VDX 6730 switch for use as an ISL (inter-switch link) or an ICC (inter-cluster communication) switch.
- *Best Practices for Hitachi NAS Universal Migrator (MK-92HNAS047)*—The Hitachi NAS Universal Migrator (UM) feature provides customers with a
convenient and minimally disruptive method to migrate from their existing NAS system to the Hitachi NAS Platform. The practices and recommendations outlined in this document describe how to best use this feature.

- *Hitachi NAS Platform Storage Pool and HDP Best Practices* —This document details the best practices for configuring and using HNAS storage pools, related features, and Hitachi Dynamic Provisioning (HDP).
File systems formatted as WFS-2 offer several improvements over file systems formatted using the older WFS-1 format. These benefits include:

- Fast file system roll back to a specific checkpoint.
- Fewer disks are required to achieve a given level of performance in file systems that have a high churn rate. The churn rate is higher when file systems perform intensive file system object modifications, such as creating new files and directories, deleting files and directories, or changing the content of files.
- Tiered file systems formatted using WFS-2 can expand either tier as necessary, up to their defined size limit, as long as space is available. If a tiered file system is formatted using WFS-1, the server will not distinguish between tiers, meaning that the server will not place metadata on Tier 0 and user data on Tier 1. Furthermore, any auto-expansion will draw space from Tier 1, and the server will not expand Tier 0.
- The writable clone feature, which provides a mechanism for the quick copying of files. The “clones” are writable snapshots of the original (master) file, and they do not use additional storage space unless they become different from the master file, and then only the changed data blocks are duplicated.
- Support for deduplication is supported only on file systems formatted as WFS-2. Deduplication offers the following benefits:
  - Identifies and removes duplicate blocks of data while maintaining a reference to the original data.
  - Eliminates duplicates, while maintaining a single copy of the data along with references to the single copy.
  - All data in the specified file system are scanned at intervals and duplicate blocks removed, resulting in reclaimed disk space.

**Note:** By default, when WFS-2 is supported by the hardware platform, all new file systems are formatted using the WFS-2 format, but file systems previously created using the WFS-1 format can still be mounted and used.
- File system tiers
- Tiered file systems and snapshots
- Creating a normal file system
- Read caches
- WORM file systems
- Deduplication file systems
- Cloning files
**File system access protocols**

The server supports the CIFS, NFS, and FTP protocols for client file access, as well as iSCSI for block-level access to storage. All supported protocols can be enabled or disabled.

The server allows NFS, CIFS, and FTP users to access the same file space; however, although iSCSI Logical Units (LUs) reside on file systems, it is not possible to access folders and files located on an iSCSI target through the server’s file services (for example, CIFS or NFS).

These protocols, with the exception of FTP, require a license key for activation.

**File system tiers**

A file system typically consists of files and directories. Data about the files and directories (as well as many other attributes) is kept; this information is the metadata. The data within the file system (both user data and metadata) is stored on the storage media of a storage subsystem.

Different storage subsystems have varying characteristics, in terms of both performance and cost. Based on their performance, storage subsystems are classified into “tiers,” which are then used by administrators to manage the storage resources in the organization.

Storage pools can be created using storage from different tiers (up to two tiers are currently supported). These storage pools are called tiered storage pools. File system data (metadata and user data) may be stored in a single tier, or in multiple tiers. When file system data is stored on storage subsystems on multiple tiers, the file system is called a tiered file system.

For more information on storage tiers and tiered storage pools, refer to the *Storage Subsystem Administration Guide*.

In a tiered file system, metadata is stored on the highest performance tier of storage, and user data is stored on a lower-performance tier. A tiered file system may provide the following:

- **Performance benefits:** Storing metadata on the higher-performance tier provides system performance benefits over storing both the metadata and user data on the same, lower, tier of storage. The performance gain is seen because metadata is accessed more often than the user data, so storing it on higher-performance storage increases overall performance.
- **Reduced expenses for storage:** Storing metadata on the higher-performance storage (which is usually more expensive than the lower performance storage) and user data on lower performance (and less expensive) storage may provide cost benefits. This is because metadata
typically consumes a relatively small amount of storage, while the user data consumes the bulk of the storage. Because the higher-performance storage is used only to hold the metadata, less of the expensive storage is used than if both the metadata and the user data were on the higher-performance storage. Also, because user data can be kept on lower performance storage while achieving better performance than keeping both metadata and user data on the lower performance storage, you may not have to upgrade storage as often (or you may be able to repurpose aging storage when you do upgrade).

Note: If a tiered file system was formatted using the WFS-1 file system format, the server will not distinguish between tiers, meaning that the server will not place metadata on Tier 0 and user data on Tier 1. This means that the benefits of using a tiered file system will not apply to file systems formatted using the WFS-1 file system format. When formatting a tiered file system, only the WFS-2 format is supported, and formatting the file system using the WFS-1 format is no longer supported. Existing tiered file systems that were formatted using WFS-1 may still be mounted and used.

A tiered file system has the following characteristics:

- Maintains a single file system view while providing data separation. This separation allows the file system to store file system metadata (which is critical to system performance) on very high-performance devices, while storing user data on cheaper, lower-performance storage subsystems.
- The use of multiple tiers of storage is completely transparent to applications or clients. No environmental tweaking or effort is required. All file system functionality (such as snapshots, replication, quotas, cluster name space, and virtual volumes) is preserved.
- File system management activities, such as mounting, unmounting, sharing, and exporting, for tiered file systems are the same as for untiered file systems.
- The file system block size (4 KB or 32 KB) is maintained across all tiers of storage.
- Cross volume links are treated as metadata.

**Tiered file systems and snapshots**

Snapshots preserve changed blocks in place. With tiered file systems, this means that snapshots of metadata are preserved in Tier 0 (the "expensive" storage tier). Space will eventually be reclaimed when snapshots are deleted.

While snapshots normally take a relatively small proportion of disk space, snapshots of metadata may take up a larger proportion of space. Should the file system run out of space in the expensive storage tier, metadata will be allocated elsewhere in the file system.
Creating a normal file system

This procedure creates a new file system. A storage pool is required before a file system can be created.

**Note:** If Dynamic Write Balancing is not enabled, or if your system does not support Dynamic Write Balancing, when expanding a storage pool, use as many disk drives as possible and keep SDs as large as possible to attain optimal performance. For more information on Dynamic Write Balancing, refer to the *Storage Subsystem Administration Guide*.

**Procedure**

1. From the Home page, navigate to **Storage Management > File Systems** to display the **File System** page.
2. Click **create** to display the **Create File System** page.
3. Click **File System**.
4. Select the required storage pool, and then click next to start the Storage Pool Wizard.

   For more information about the Storage Pool Wizard, refer to the *Storage Subsystem Administration Guide*.  

...
5. Select a storage pool to contain the file system, then click **next** to display the **Create File System** page.

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Pool</td>
<td>Displays the name of the storage pool in which the file system or read cache is being created.</td>
</tr>
<tr>
<td>Free Capacity Amount</td>
<td>Displays the available space in the storage pool that can be used by the file systems.</td>
</tr>
<tr>
<td>Tier 0 Meta-data and Tier 1 User-data</td>
<td>Displays the size of the storage pool’s metadata tier (Tier 0) and the user data tier (Tier 1).</td>
</tr>
<tr>
<td>Guideline Chunk Size</td>
<td>Displays the approximate size of the chunks used in the selected storage pool.</td>
</tr>
</tbody>
</table>
| Size Limit                  | If Auto-Expansion is enabled:  
  - For an untiered file system, this is the maximum size to which a file system will be allowed to expand.  
  - For a tiered file system this is the maximum size to which the user data tier (Tier 1) of the file system will be allowed to expand.  
  If Auto-Expansion is disabled:  
  - Specifies the capacity with which the new file system should be created. The file system will be created and this amount of }
6. **Enter a Size Limit** for the file system.
This defines the maximum size to which the file system or user data tier can grow through Auto-Expansion. Once the file system has been created, this value can be changed on the **File System Details** page. This limit is not enforced for manual file system expansions performed through the CLI.

7. The value in the **Rounded Size Limit** field is calculated automatically, but can be changed. For more information, click **Rounded to nearest chunk**. If the specified size is not a multiple of the chunk size, the server rounds down to the nearest chunk boundary.

8. Use these radio buttons to **enable** or **disable** Auto-Expansion, which allows or constrains growth of this file system or user data tier (for tiered file systems).

Be aware that storage pools can be configured to prevent the growth of file systems. A file system can never shrink; once space is allocated to a
file system, the space cannot be recovered, and the file system cannot be reduced in size. When expanding, the file system will use the storage pool’s chunk size as its growth increment. File systems configured to automatically expand will do so when they are about 80 percent full. File systems can be expanded manually through the CLI. File system expansion does not interrupt file services or require the file system to be unmounted.

9. In the **Initial Capacity** field, set the initial size for the file system or user data tier.

10. In the **Label** field, enter the name of the file system.
    File system labels are not case sensitive, but they do preserve case (labels will be kept as entered, in any combination of upper and lowercase characters). Also, file system labels cannot contain spaces or any of the following special characters: "&'*/;:<>?\]. File system labels must be unique within a server or cluster. Also, a file system cannot have the same label as a storage pool.

11. From the EVS list, select the **EVS** to which the file system should be assigned.

12. Fill in the **Object Replication Target** check box if the file system is intended to be the target of an object replication. When this check box is filled, the file system will be formatted to allow shares and exports.

13. Fill in the **Support and Enable Dedupe** check box to support and enable deduplication on the file system.

**Note:** Support for dedupe applies to WFS-2 files systems only.

14. In the **Block Size** field, enter the desired file system block size.

15. Click **OK**.

### Read caches

A read cache is a special read-only file system that stores copies of individual files outside of their local file systems, enabling a server or a node to have a cached copy of the file. When NFS v2 or NFS v3 clients submit a read request for a file in the read cache, the server or node can serve the read request from the copy in the read cache. Note that a read cache does not benefit CIFS clients, and that read caches have special characteristics and limitations. For information about read caches, refer to the *Storage Subsystem Administration Guide*. 
WORM file systems

The storage server supports Write Once Read Many (WORM) file systems. WORM file systems are widely used to store crucial company data in an unalterable state for a specific duration.

Note: A license is required to use WORM file systems. Contact your Hitachi Data Systems representative to purchase a WORM license.

The server supports two types of WORM file systems: strict and non-strict:
• Strict WORM file systems cannot be deleted or reformatted and should be used once strict compliance measures are ready to be deployed.
• Non-strict WORM file systems can be reformatted and so should only be used for testing purposes. Should a non-strict WORM file system need to be deleted, it must first be reformatted as a non-WORM file system.

Caution: WORM file systems should be created only if you need to use the file system for regulatory compliance purposes to ensure that your company’s data retention policies comply with government regulations.

WORM file system characteristics

WORM file systems have several very important characteristics that differentiate them from regular file systems:
• No changes once marked WORM. Network clients can access files on a WORM file system in the same way they access other files. However, once a file is marked as WORM, it is “locked down.” WORM files cannot be modified, renamed, deleted, or have their permissions or ownership changed. These restrictions apply to all users including the owner, Domain Administrators, and ‘root.’
• Once a WORM, always a WORM. Once marked as WORM, the file remains a WORM file until its retention date has elapsed. In contrast, files not marked as WORM can be accessed and used just as any normal file.
• You can expand and add more storage to a WORM file system, but you cannot reclaim unused space, and you cannot delete the WORM file system. Also, just like any non-WORM file system, you cannot shrink a WORM file system, or reclaim unused space, and you cannot delete the WORM file system.

Note: WORM file system types can only be created through the CLI. See the man pages for details.
Deduplication file systems

Deduplication is a file system feature that incorporates enhancements to the file system and the HNAS application layer. Deduplication features the ability to reduce redundancy in stored data blocks. All data in the specified file system is scanned at intervals and duplicate blocks are removed, resulting in reclaimed disk space. All dedupe activity and the elimination of redundant blocks is transparent to the user.

Base deduplication is enabled by default and does not require a license key. This is a dedupe feature with a single SHA-256 engine, capable of indexing data at a rate of up to 120 MB per second.

The Premium deduplication is a licensed feature and must be installed before deduplication can be performed. This is a dedupe feature with a four SHA-256 engines, capable of indexing data at a rate of up to 450 MB per second. Contact your Hitachi Data Systems representative for more information.

For license key information, see the Server and Cluster Administration Guide.

Deduplication characteristics

Deduplication is a file system feature that incorporates enhancements to the file system and the HNAS application layer. Data deduplication software identifies duplicate data blocks in order to remove redundancy.

- Only user data blocks are deduplicated.
- Dedupe is a post-process that is performed as a fixed block-based deduplication. The process is not an inline dedupe process.
- Data is deduped within a given a file system and not across multiple file systems.

Dedupe has been intelligently designed with quality of service (QoS) as a key component. File system activity will take precedence over dedupe activity when file serving load goes beyond 50 percent of the available IOPS or throughput capacity. The deduplication process throttles back to allow the additional file serving traffic load to continue without impacting performance.

- You can configure a new file system to support and enable dedupe.
- An existing WFS-2 file system can be converted to be dedupe-enabled.
- File systems with support for dedupe can be dedupe-enabled or dedupe-disabled.

Deduplication interoperability with existing Hitachi NAS Platform features

The following table lists the HNAS applications that are compatible with Dedupe.
## Calculating Dedupe space savings

The `df` command reports the amount and the percentage of data that was deduped. The following example describes how the dedupe space savings is calculated.

If the difference between physical and logical space of 100 TB of data before deduplication:

- **Group A:** 30 TB of distinct data
- **Group B:** 70 TB of duplicated data that contains only 10 TB of unique data blocks.
  - Given an arbitrary data block in Group B, there may be one or more identical data blocks in Group B, and not in Group A, but an arbitrary data block in Group A has no identical data block in either groups.

If both Group A and Group B have gone through the dedupe process:

- Group A had no duplicates removed and consumed the same 30 TB.
- Group B had duplicates removed and consumed only 10 TB to hold the unique data blocks.
• Group B (70 TB) = \{Group C (10 TB raw remaining)\} + \{Group D (60 TB deduped and now sharing or pointing to physical blocks of group C)\}
• The original 100 TB of data now requires only 40 TB (30 plus 10) of physical blocks because all duplicates were removed. However, the logical data size is 100 TB (30 plus 70), which is the amount of space needed if the data were not deduped. The results are outlined in the following table:

<table>
<thead>
<tr>
<th>Used Space</th>
<th>The amount of physical disk space used by the file system, in this example, group A and group C = 30 + 10 = 40 TB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dedupe space</td>
<td>The amount of duplicate data that does not occupy its own physical disk space, but has been deduped to share existing physical blocks = group D = 60 TB</td>
</tr>
<tr>
<td>Logical space</td>
<td>The amount of physical disk space that would be required if the data were not deduped = {used space} + {deduped space} = 40 + 60 = 100 TB</td>
</tr>
</tbody>
</table>

Based on the example presented, the deduped percentage gives the amount of physical disk space saved by removing the duplicates. The percentage measures against the amount of space that would be required if the data were not deduped:

\[
\text{Dedupe Percentage} = \frac{\text{Dedupe}}{\text{Logical}} = \frac{\text{Dedupe}}{\text{Used+Dedupe}} = \frac{60}{40+60} = 60\%
\]

Viewing deduped file system usage

The `df` command reports the amount and the percentage of data that was deduped. The Deduped column reports the amount of data that has been deduped in the file system, which is the amount of disk space that was saved by dedupe. For example:

<table>
<thead>
<tr>
<th>ID</th>
<th>Label</th>
<th>Size</th>
<th>Used Snapshots</th>
<th>Deduped</th>
<th>Avail</th>
<th>Thin</th>
<th>ThinSize</th>
<th>ThinAvail</th>
<th>FS Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1010</td>
<td>mfsfa</td>
<td>1.27 TB</td>
<td>541 GB (44%)</td>
<td>667 GB (54%)</td>
<td>797 GB (67%)</td>
<td>No</td>
<td></td>
<td>420 MB</td>
<td>NFS (Uses 8192 MB)</td>
</tr>
</tbody>
</table>

• All columns except Snapshots and Deduped have the same meaning as a normal file system:
  o Size column: The formatted capacity of the file system.
  o Used column: The amount (and percentage) of formatted capacity used by live and snapshot data.
  o Avail column: The amount of formatted capacity available for further data.
• **Deduped column**  
  ○ This column reports the amount (and percentage) of deduped data in the file system.

• **Snapshots column**  
  ○ This column normally reports the amount (and percentage) of logical space used by snapshots.  
  ○ On file systems that do not support dedupe, the logical size of data is equal to the physical space used by that data. However, on file systems that support dedupe, the logical space used by snapshots can exceed the physical used size due to block sharing through Dedupe.  
  ○ In some cases, snapshot space usage can even exceed the total formatted capacity of file system size. To avoid confusion, the Snapshots column displays NA for file systems that support dedupe.

**Cloning files**

Furthering the capabilities of WFS-2 file systems, two types of cloning are available:  
• File cloning  
• Tree directory cloning

The **file clone** feature allows for the quick copying of a file, which is space efficient when the source file and its copies ("clones") do not diverge significantly from each other over time. This feature is intended for situations in which long-lived and mostly unchanging copies of a large master file are required (for example, deploying many copies of an OS disk image for virtualized desktops). When a file clone is created, a snapshot of the master file is created, preserving an image of the source file at that point in time. The snapshot is only of the file, it is accessible only by the NAS server, and it is read-only. This snapshot allows the source file and clone to share common data blocks. If additional clones of the master file are created, new snapshots are created if necessary.

The maximum number of clones is based on available resources, and file cloning is not space efficient when the related clones diverge significantly from each other. If some clones are short-lived and others are long-lived, the overall space efficiency of file clones is reduced because the data blocks that were once shared between clones are not freed until all related clones and the source (master) file, are deleted.

The **tree directory cloning** feature provides a way to quickly create space efficient writeable copies of a directory tree. Space-efficiency is achieved by creating clones of the source files in the destination tree. This space-efficiency will reduce as the source files and its clones diverge over time. The source directory’s structure is recreated in the destination directory and all of the contained files are cloned. Security information from the source files and directories are applied to the destination. The source directory can be
modified while tree cloning is in progress, and the cloned destination is not a point-in-time replica. Tree cloning uses the same mechanism as file cloning to clone individual files within the tree, so the same limitations apply.

A FileClone license is required to enable the clones features.

Notes: File cloning and tree directory cloning is supported only for files in file systems formatted using WFS-2; cloning files in a WFS-1 file system is not supported. Additionally, file cloning is supported on all Hitachi NAS Platform models.

After this feature has been used, certain downgrade restrictions will apply. If you downgrade to a release that does not support file clones, file systems on which file cloning has been used cannot be mounted. Contact Hitachi Data Systems Support Center for more information about downgrade restrictions when using file clones.

File clone commands

Currently Web Manager does not include support for file cloning; to use this feature, you must use CLI commands. See the following CLI man pages for detailed information on configuring and using the file clone feature:

- `file-clone`
  Provides a description of the file cloning mechanism.

- `file-clone-create`
  Creates a new file, and makes its data stream a clone of the source file’s data stream.

- `file-clone-stat`
  Displays statistics regarding a clone object; specifically, the handles of the snapshot file objects on which it depends.

- `file-clone-report-block-sharing`
  Reports on the amount of block sharing between a clone and each of its predecessor snapshot file objects.

- `file-clone-declone`
  Removes the dependency of a cloned file from its snapshot object, converting the clone into a normal file.

- `file-clone-stat-snapshot-file`
  Displays statistics regarding a snapshot file object.

Tree clone commands

Currently Web Manager does not include support for tree cloning; to use this feature, you must use CLI commands. See the following CLI man pages for detailed information on configuring and using the tree clone feature:

- `tree-clone-job-submit`
  Submits a request to clone a directory tree.

- `tree-clone-job-status`
Gets the status of a tree cloning job specified by its job id.

- **tree-clone-job-list**
  Lists the status of tree cloning jobs.

- **tree-clone-job-abort**
  Aborts a tree cloning job specified by its job id.
Managing file system performance

You can manage the file system performance by using per-file system throttling (PFST) commands. PFST allows you to place an upper limit on resource usage on a particular file system, which prevents a file system from using too many server resources. All PFST commands take effect on a cluster-wide basis.

- Using the per-file system throttle feature
- Creating a read cache file system
- Viewing available file systems
- Displaying file system details
- Formatting a file system
- Mounting a file system
- Unmounting a file system
- Deleting a file system
- Undeleting a file system
- Tree directory delete
- Controlling file system space usage
Using the per-file system throttle feature

To use the per-file system throttle feature, you must have Dev User access rights. The PFST feature allows you to:

- Enable and disable a PFST.
- List the PFST properties, including quota and number of queued operations.
- Create, delete, and modify PFST classes.
- Maintain mappings of file systems to PFST classes.

The following table lists the CLI commands to enable, disable, create, delete, and modify the per-file system throttle feature. For more information on a specific command, refer to the CLI man page.

<table>
<thead>
<tr>
<th>Description</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>To enable a per-fs-throttle bossock fiber quota</td>
<td><code>per-fs-throttle-class-enable</code></td>
</tr>
<tr>
<td>To disable a per-fs-throttle bossock fiber quota</td>
<td><code>per-fs-throttle-class-disable</code></td>
</tr>
<tr>
<td>To create a per-file system throttle class</td>
<td><code>per-fs-throttle-class-create</code></td>
</tr>
<tr>
<td>To delete a per-file system throttle class</td>
<td><code>per-fs-throttle-class-delete</code></td>
</tr>
<tr>
<td>To modify a per-file system throttle class</td>
<td><code>per-fs-throttle-class-set</code></td>
</tr>
</tbody>
</table>

Creating a read cache file system

A read cache is a special read-only file system that stores copies of individual files outside of their local file systems, enabling a server or a node to have a cached copy of the file.

Procedure

1. From the Home page, navigate to **Storage Management > File Systems** to display the **File System** page.
2. Click **Read Cache**.
3. Select a storage pool to contain the read cache, and then click next to display the Create Read Cache page.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Pool</td>
<td>Displays the name of the storage pool in which the read cache file system is being created.</td>
</tr>
<tr>
<td>Free Capacity Amount</td>
<td>Displays the available space in the storage pool that can be used by read cache file systems.</td>
</tr>
<tr>
<td>Tier 0 Meta-data and Tier 1 User-data</td>
<td>Displays the size of the storage pool's metadata tier (Tier 0) and the user data tier (Tier 1).</td>
</tr>
<tr>
<td>Guideline Chunk Size</td>
<td>Displays the approximate size of the chunks used in the selected storage pool.</td>
</tr>
<tr>
<td>Size</td>
<td>The size of the read cache being created. Enter a size for the read cache.</td>
</tr>
<tr>
<td></td>
<td>- For an untiered read cache, this defines the total size of the read cache.</td>
</tr>
<tr>
<td></td>
<td>- For a tiered read cache, this defines the size of the user-data tier of the read cache.</td>
</tr>
</tbody>
</table>
4. Enter a **Size Limit** for the file system.
   This defines the maximum size to which the file system or user data tier can grow through Auto-Expansion. Once the file system has been created, this value can be changed on the File System Details page. This limit is not enforced for manual file system expansions performed through the CLI.

5. The value in the **Rounded Size Limit** field is calculated automatically, but can be changed. For more information, click **Rounded to nearest chunk**. If the specified size is not a multiple of the chunk size, the server rounds down to the nearest chunk boundary.

6. In the **Label** field, enter the name of the file system.
   File system labels are not case sensitive, but they do preserve case (labels will be kept as entered, in any combination of upper and lowercase characters). Also, file system labels cannot contain spaces or any of the following special characters: "&'/*;:<>!?". File system labels must be unique within a server or cluster. Also, a file system cannot have the same label as a storage pool.

7. From the EVS list, select the **EVS** to which the file system should be assigned.

8. In the **Block Size** field, enter the desired file system block size.

9. Click **OK**.
Viewing available file systems

Procedure

1. Navigate to **Home > Storage Management > File Systems** to display the **File Systems** page.

### Field/Item Description

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Filter** | Click to open the Filter dialog box and enter one or more of the following filtering criteria:  
  - File System  
  - Storage Pool  
  - Status  
  - EVS  
  File Systems that meet the specified criteria are displayed on the page. |
| **Label** | Name of the file system, assigned upon creation and used to identify the file system when performing particular operations; for example, creating an export or taking a snapshot. |
| **Total** | Size of the file system. |
| **Used** | Amount of space used.  
  The following Usage Alerts criteria apply:  
  - If Usage Alerts are enabled on the entire file system, the sliding bar turns yellow when the warning limit is exceeded and orange when the severe limit is exceeded. |
<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• If Usage Alerts are not enabled, the sliding bar turns yellow when 85% capacity is reached and orange when the file system is full.</td>
<td></td>
</tr>
<tr>
<td>Free</td>
<td>Amount of free space available (GB).</td>
</tr>
<tr>
<td>Storage Pool</td>
<td>Name of the storage pool on which the file system resides.</td>
</tr>
</tbody>
</table>
| Status | **Checking**: The file system is being checked; during this check, the approximate percentage of completion for each phase of the check (note that some phases take longer than others, and that the percentage complete is only for the current phase, not for the overall procedure).  
**Failing**: The file system has failed, but is being checked, fixed, or recovered.  
**Fixing**: The file system is being repaired. When fixing, an approximate percentage complete is displayed for each phase of the repair (note that some repair phases take longer than others, and that the percentage complete is only for the current phase, not for the overall procedure).  
**Formatting**: The file system is being formatted. |
| EVS | EVS to which the file system is assigned. |
| details | Displays the File System Details page for the selected file system. |
| mount | Select one or more unmounted file systems and click mount to mount the file system.  
**Note**: The server remembers which file systems were mounted when it shuts down, and mounts them automatically during system startup. |
Displaying file system details

Procedure

1. Navigate to **Home > Storage Management > File Systems**.
2. Select a file system and click **details** to display the **File System Details** page.

The following table describes the fields in this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Settings/Status</strong></td>
<td></td>
</tr>
<tr>
<td>Label</td>
<td>Name of the file system, assigned upon creation and used to identify the file system when performing particular operations; for example, creating an export or taking a snapshot.</td>
</tr>
<tr>
<td>Capacity</td>
<td>Displays information about the space allocation and usage for the file system. For a tiered file system, information about both the metadata and user data tiers is displayed. For an untiered file system, information about the total size of the file system is displayed.</td>
</tr>
<tr>
<td>% Total Used Space</td>
<td>Percentage of the file system's total allocated space that has been used. This total reflects data and snapshots, if any.</td>
</tr>
<tr>
<td>Capacity</td>
<td>Total amount of formatted space (free + used space).</td>
</tr>
<tr>
<td>Free</td>
<td>Total amount of file system space unused (free), in GB and as a percentage of the total.</td>
</tr>
<tr>
<td>Total Used</td>
<td>Total amount of file system space in use, in GB and as a percentage of the total.</td>
</tr>
<tr>
<td>Field/Item</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Live File System</strong>: Total space used by the file system data, in GB and as a percentage of the total.</td>
<td></td>
</tr>
<tr>
<td><strong>Snapshots</strong>: Total space used by snapshots of the file system, in GB and as a percentage of the total.</td>
<td></td>
</tr>
</tbody>
</table>

**Note**: These areas are displayed only for tiered file systems.

These areas display information about the space allocation and usage for the tiers making up the file system. The Tier 0 Meta-data section describes information about the metadata tier. The Tier 1 User-data section describes information about the user data tier.

- **% Total Used Space**: Percentage of the file system’s total allocated space that has been used. This total reflects data and snapshots, if any.
- **Capacity**: Total amount of formatted space (free + used space).
- **Free**: Total amount of file system space unused (free), in GB and as a percentage of the total.
- **Total Used**: Total amount of file system space in use, in GB and as a percentage of the total.
- **Confine Auto-Expansion to**: Indicates the maximum capacity of the tier (including metadata/user data and snapshots). When the original allocation of storage for the tier is used, auto-expansion of the tier occurs up to this limit.

If you change any of the auto-expansion limits, click **apply** to make the changes effective.

### Configuration

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status</strong></td>
<td>Current status of the file system, showing whether the file system is mounted or unmounted.</td>
</tr>
<tr>
<td><strong>Syslock</strong></td>
<td>Indicates whether the file system is in Syslocked mode (System Lock enabled), or if the file system is not in Syslocked mode (System Lock disabled). When System Lock is enabled for a file system, NDMP has full access to the file system and can write to it during a backup or replication, but the file system remains in read-only mode to clients using the file service protocols (NFS, CIFS, FTP, and iSCSI). To enable/disable the System Lock for a file system, click <strong>enable</strong> or <strong>disable</strong>. When viewing the details of a read cache, the System Lock’s enable/disable button is not available.</td>
</tr>
<tr>
<td><strong>Object Replication Target</strong></td>
<td>Indicates whether or not the file system is formatted as an object replication target. A file system must be formatted as an object replication target in order to be the target of a replication.</td>
</tr>
<tr>
<td><strong>Transfer Access Points During Object Replication</strong></td>
<td>Indicates whether or not the file system is enabled to allow transfer access points during an object replication. If disabled, click enable to allow the file system to transfer access points during an object replication.</td>
</tr>
<tr>
<td>Field/Item</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>replication</td>
<td>If enabled, click disable to prohibit the transfer of access points during an object replication.</td>
</tr>
<tr>
<td>Deduplication</td>
<td>Indicates whether or not the file system is enabled or disabled for a file system with support for dedupe.</td>
</tr>
<tr>
<td>EVS</td>
<td>EVS to which the file system is assigned. If the file system is not currently assigned to an EVS, a list of EVSs (to which the file system can be assigned) appears.</td>
</tr>
<tr>
<td>Security Mode</td>
<td>Displays the file system security policy defined for the file system.</td>
</tr>
<tr>
<td>Block Size</td>
<td>File system block size: 32 KB or 4 KB, as defined when the file system was formatted.</td>
</tr>
<tr>
<td>Read Cache</td>
<td>Indicates whether this file system is a read cache (Yes) or a regular file system (No).</td>
</tr>
<tr>
<td>WFS Version</td>
<td>Indicates whether this file system has been formatted as a WFS-1 file system or a WFS-2 file system.</td>
</tr>
</tbody>
</table>

**Auto-expansion**

<table>
<thead>
<tr>
<th>Confine Auto-Expansion to</th>
<th><img src="https://example.com" alt="Note: This section is displayed only for untiered file systems. For tiered file systems, this information is incorporated in the Tier 0 Meta-data and Tier 1 User-data sections of this page." /></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Indicates the maximum capacity of the tier (including metadata/user data and snapshots). When the original allocation of storage for the tier is used, auto-expansion of the tier occurs up to this limit.</td>
</tr>
<tr>
<td></td>
<td>If you change the auto-expansion limit, you must click apply to make the changes effective.</td>
</tr>
</tbody>
</table>

**Usage Thresholds**

<table>
<thead>
<tr>
<th>File System Usage</th>
<th>Usage thresholds are expressed as a percentage of the space that has been allocated to the file system.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>When a threshold is reached, an event is logged and, depending on quota settings, an email may be sent. This area displays information on current usage for each of the following:</td>
</tr>
<tr>
<td></td>
<td>• Live file system (data).</td>
</tr>
<tr>
<td></td>
<td>• File system snapshots.</td>
</tr>
<tr>
<td></td>
<td>• Total of the live file system data and snapshots.</td>
</tr>
<tr>
<td></td>
<td>You can use the edit boxes to specify the Warning and Severe thresholds:</td>
</tr>
<tr>
<td></td>
<td>• The Warning threshold should be set to indicate a high, but not critical, level of usage.</td>
</tr>
<tr>
<td></td>
<td>• The Severe threshold should be set to indicate a critical level of usage, a situation in which an out-of-space condition may be imminent.</td>
</tr>
</tbody>
</table>
You can define both Warning and Severe thresholds for any or all of the following:
- Live file system (data).
- File system snapshots.
- Total of the live file system and snapshots.

To verify that the live file system does not expand beyond its Severe threshold setting, which would cause snapshots to be lost, fill the **Do not allow the live file system to expand above its Severe limit** check box.

### Associations

**Storage Pool**
The name of the storage pool in which the file system or read cache was created.

This area also displays the following information:
- **Capacity**: The total space allocated to the storage pool.
- **Free**: The total storage pool free space, in MB, GB or TB, and as a percentage of the total.
- **Used**: The total storage pool used space, in MB, GB or TB, and as a percentage of the total.

**Related File Systems**
Displays the name of any related file systems. A related file system is one that is either the:
- Source of a migration or replication operation where this file system was the target of the operation.
- Target of a migration or replication operation where this file system was the source of the operation.

If there are related file systems, the date of the last successfully completed operation (migration or replication), if any, is displayed.

### Check/Fix

**Status**
Indicates when the file system was last checked, and displays its status since its last reboot. File system status messages may be any of the following:
- File system is not being checked or fixed.
- Checking.
- Fixing.

You can start a check of the file system, or just part of the file system, using the Scope settings and the browse and check buttons.

If one or more checks is in progress, click **Active Tasks** to view the **Active Tasks** page for more information about active tasks.

**Scope**
The scope controls allow you to set the scope of a check by the entire file system or the directory tree.

To check the whole file system, click the **Entire File System** radio button.

To check a part of the file system, click the **Directory Tree** radio button, then use the browse button to navigate to the part of the file system you want to check.

Once you have set the scope, click **check** to start the check.

**mount**
Use to mount the file system.
### Formatting a file system

Formatting a file system prepares it for use by clients for data storage. File systems created through the Web UI will be formatted and mounted automatically. Therefore, this procedure should rarely, if ever, be used.

**Important:**
- After a file system has been deleted, it can still be undeleted *if it is still in the recycle bin.*
- Freed chunks move to a vacated-chunks-list. See the CLI man pages for details.
- Vacated chunks are reused when you create or expand other storage pools.
- You must be either a Global Admin or Storage Admin, and must have Advanced Mode enabled to delete a file system. For more information, refer to the *Storage System User Administration Guide*.
- This procedure assumes that the file system has already been mounted.

**Procedure**

1. From the Home page, navigate to **Storage Management > File Systems** to display a list of all file systems.
2. For the file system to be formatted, click **details**.
3. If the file system is mounted, do the following to unmount it; otherwise, skip to **Formatting a file system on page 41**.
   a. From the Label column, select the file system.
   b. From the Actions section, click **unmount**.
c. In the confirmation dialog, click OK.
4. Click format to display the Format File System page.
5. Use the radio buttons to select 32 KB or 4 KB as the block size for the file system.
6. If the file system will be the target of an object replication, fill the Object Replication Target checkbox. If the file system will not be the target of an object replication, make sure the Object Replication Target checkbox is empty.
   A file system must be formatted as an object replication target in order to be the target of a replication. When this check box is filled, the file system will be formatted to allow shares and exports.
7. Click OK to format the file system and return to the File System details page.

**Mounting a file system**

Use this procedure to manually mount a file system. Mounting a formatted file system makes it available to be shared or exported, and thus accessible for use by network clients. This procedure may also be used when an auto-mount of a file system has failed, which can occur in the following situations:

- The file system was not mounted when the server was shut down.
- The command line interface was used to disable auto-mounting.
- A storage system failure caused the server to restart.

**Procedure**

1. Navigate to Home > Storage Management > File Systems to display a list of all file systems.
2. Fill the check box next to the label of the file system to be mounted.
3. If the file system is unmounted, click mount.

**Unmounting a file system**

Unmount a file system when it needs to be removed from service. From a client point of view, it simply disappears. This will not harm the file system, nor affect any of the data in it.

**Note:** You do not need to unmount a file system before shutting down or restarting a server or cluster. If a file system was mounted when the server or cluster was shut down or restarted, the file system will automatically be mounted when the server or cluster is restarted.

**Procedure**

1. Navigate to Home > Storage Management > File Systems to display a list of all file systems.
2. Fill the check box next to the label of the file system to be unmounted.
3. If the file system is mounted, click unmount.
4. Click OK.

Deleting a file system

You can delete a file system at any time, unless it is a strict WORM file system. After a file system has been deleted, the free space is restored to its storage pool.

Important:
- After a file system has been deleted, it can still be undeleted if it is still in the recycle bin.
- Freed chunks move to a vacated-chunks-list. See the CLI man pages for details.
- Vacated chunks are reused when you create or expand other storage pools.
- You must be either a Global Admin or Storage Admin, and must have Advanced Mode enabled to delete a file system. For more information, refer to the Storage System User Administration Guide.

Procedure

1. Navigate to Home > Storage Management > File Systems to display a list of all file systems.
2. For the file system to be deleted, click details.
3. If the file system is mounted click unmount and click OK. If the file system is unmounted, skip this step.
4. In the Actions section, click delete and click OK.

Undeleting a file system

When you delete a file system, it spends some time in the span's recycle bin before being recycled (permanently destroyed). As long as it is in the recycle bin, you can use filesystem-undelete to undelete it. After a period of time (about seven days, or sooner if space is needed by other file systems) the recycle bin is automatically recycled and you can no longer use the filesystem-undelete command to bring back a file system.

The filesystem-undelete command was introduced in release 12.0. Earlier releases do not maintain a recycle bin; therefore, if a file system was deleted under an earlier software release, you cannot upgrade to 12.0 and then use 'filesystem-undelete' to undelete it.

In release 12.1, after a file system has been deleted and the time in the recycling bin has passed, the freed chunks are moved to a vacated-chunks
list (VC list), which is stored in Cod. The vacated chunks are reused when you create or expand other spans. Reuse of the chunks avoids premature exhaustion of space and prevents the back up of recycled file systems with real disk storage.

This command and the recycle bin are described more fully in the man pages. You can only use this command from the CLI.

**Tree directory delete**

The **tree delete** feature provides a mechanism to immediately remove a directory tree from its position in the file system and to perform the deletion as a background job. A directory tree consists of a specified directory and the hierarchy of subdirectories and files below it. When a directory tree is targeted for deletion, a **tree delete** job is created and added to the job queue. The targeted directory tree is immediately removed from the file system namespace, moved to the system trash directory, and scheduled for background deletion.

The **Tree delete** interfaces are provided in the form of management APIs, new CLI commands, and SOAP interfaces. **Tree delete** is supported on WFS-2 file systems. No license is required.

The **tree delete** feature provides the following benefits, compared to deleting a directory tree via a network client:

- The instantaneous removal of a directory tree from the listing of the parent directory, allowing the client to proceed with further actions.

- The server-side delete eliminates the need for a client to recursively delete the directory tree over the network, therefore using less system resources.

- The multi-threaded implementation allows parallel deletion of the contents of the directory tree.

**Important considerations when using tree delete**

The **tree delete** SOAP APIs can destroy user data, and the **feature should only be invoked with great care**. Note that, although the targeted directory tree is immediately removed from the file system namespace and the listing of the parent directory, the client will continue to have access to parts of the directory tree it had acquired access to, prior to deletion, until these parts actually get deleted in the background. Users should be mindful of the fact that changes to directory tree (creation, deletion of files/dirs) after submission for deletion will be detected by **tree-delete**, and all such new content deleted before **tree-delete** considers its job done.
Note: Quotas will only reflect the physical deletion happening in background.

Unmounting a file system and tree delete

When a file system is unmounted, all related tree-deletion activity is suspended and resumed on a subsequent re-mount.

Tree-deletion activity on other mounted file systems remains unaffected.

Undeletable directories

The following directories can not be deleted using tree delete:

- Root directory and system directories.
- Virtualization root or its sub-directory.
- Regular directory containing virtualization root(s). See the warning on deletion attempts of such a directory tree in the `tree-delete-job-submit` man page
- Sub-directory of a virtual volume.

Note: You can run `logtrace dump tree-delete` for more details about deleted files.

Maximum supported tree depth

Tree-delete supports deletion of trees maximum 1000 levels deep.

Using tree delete

Tree delete is implemented with the commands:

- `tree-delete-job-submit`
- `tree-delete-job-list`
- `tree-clone-job-submit`

Please see the man pages for details.

Submitting a tree delete job

Note the following factors when using the `tree-delete-job-submit` command:

- The main activities pertaining to a submitted `tree-delete` job, such as its start and end, are logged to the event log..
- A maximum of 160 jobs can be handled by the system at any given time.
Troubleshooting tree delete

Run `logtrace dump tree-delete` for details about deleted files. Contact customer support if necessary.

Controlling file system space usage

The server can monitor space allocation on a file system and trigger alerts when pre-set thresholds are reached; optionally, users can be prevented from creating more files once a threshold has been reached. Alternatively, the file system can be expanded either manually or automatically while online.

Two activities consume system space:

- **Live file system.** Refers to the space consumed when network users add files or increase the size of existing files.
- **Snapshots.** Refers to consistent file system images at specific points in time. Snapshots are not full copies of the live file system, and snapshot sizes change depending on the live file system. As the live file system uses more space, snapshots use more space, and as the data in the live file system is changed, snapshots require less space.

**Note:** Deleting files from the live file system may increase the space taken up by snapshots, so that no disk space is actually reclaimed as a result of the delete operation. The only sure way to reclaim space taken up by snapshots is to delete the oldest snapshot.

The server tracks space taken up by:

- The user data in the live file system
- The file system metadata (the data the HNAS server uses to manage the user data files)
- Snapshots
- Entire file system

For each of these slices, both a warning and a severe thresholds can be configured. Although they differ from system to system, the following settings should work in most cases:

<table>
<thead>
<tr>
<th></th>
<th>Warning</th>
<th>Severe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Live file system</td>
<td>70%</td>
<td>90%</td>
</tr>
<tr>
<td>Snapshots</td>
<td>20%</td>
<td>25%</td>
</tr>
<tr>
<td>Entire file system</td>
<td>90%</td>
<td>95%</td>
</tr>
</tbody>
</table>
When the storage space occupied by a volume crosses the warning threshold, a **warning** event is recorded in the event log. When the Entire File System Warning threshold has been reached, the space bar used to indicate disk usage turns yellow:

When the space reaches the severe threshold, a **severe** event is recorded in the event log, generating corresponding alerts. If the Entire File System Severe threshold has been reached, the space bar used to indicate disk usage turns amber.

If file system auto-expansion is disabled, you can limit the growth of the live file system to prevent it from crossing the severe threshold, effectively reserving the remaining space for use by snapshots. To limit the live file system to the percentage of available space defined as the severe threshold, fill the Do not allow the live file system to expand beyond its Severe limit check box on the **File System Details** page.

### Increasing the size of a file system

There are two methods to expand the amount of storage allocated to a file system:

- **Manual expansion**
  Manually expanding a file system allows you to add storage capacity to a file system (or a tier of a tiered file system) immediately. You specify the new size of a file system, and the storage is allocated immediately. The maximum size that a file system or tier can attain is specified, and the file system size can be set to the maximum size supported by the storage pool in which the file system was created.

- **Automatic expansion**
  File system auto-expansion allows a file system to grow to by adding chunks of storage on an as-needed basis, as long as the confinement limit or the maximum file system size has not been reached. For tiered file systems, auto-expansion can be applied independently to one or to all tiers of the file system, allowing one tier to expand independently of another.
  When auto-expansion is enabled, and the file system (or tier) reaches approximately 80 percent of its allocated capacity, one or more additional chunks are allocated (refer to the *Storage Subsystem Administration Guide* for a discussion of chunks). The maximum size that a file system can attain can be specified, or the file system size can be allowed to grow to the maximum size supported by the storage pool in which the file system was created.

---

**Note:** Once storage is allocated to a file system, that storage becomes dedicated to that file system, meaning that once a file system is expanded, its size may not be reduced. Unused space in the file system cannot be reclaimed, allocated to another file system, or removed. To reclaim the
storage space, the file system must be relocated to different storage or deleted.

Increasing the amount of storage allocated to a file system (manually or automatically) does not require that the file system be taken offline.

**Thin provisioning file systems**

Thin provisioning is a method of controlling how a file system's free space is calculated and reported. Administrators use thin provisioning to optimize the utilization of storage and to plan resource acquisition in a way that helps minimize expenses, while ensuring that there is enough storage for all the system needs.

Thin provisioning allows you to oversubscribe the storage connected to the storage server. As long as the available storage is not completely allocated to file systems, the oversubscription cannot be noticed by storage system users.

When thin provisioning is enabled and storage is oversubscribed, if a client attempts a write operation and there is insufficient storage space, the client will receive an insufficient space error, even though a query for the amount of free space will show that space is still available. When storage is oversubscribed, the storage server’s administrator must ensure that this situation does not occur; the storage server does not prevent this situation from occurring. To resolve this situation, the storage server’s administrator must either disable thin provisioning or add storage.

When thin provisioning is enabled, the storage server reports the amount of free space for a file system based on the file system’s expansion limit (its maximum configured capacity), rather than on the amount of free space based on the amount of storage actually allocated to the file system. Because file systems can be allowed to automatically expand up to a specified limit (the expansion limit), additional storage is allocated to the file system as needed, instead of all the storage being allocated to the file system when it is created.

For example, a file system has an expansion limit of 20 TB, with 6 TB already used and 8 TB currently allocated. If thin provisioning is enabled, the server will report that the file system has 14 TB of free space, regardless of how much free space is actually available in the storage pool. For more information about storage pools, refer to the *Storage Subsystem Administration Guide*. If thin provisioning is disabled, the server will report that the file system has 2 TB of free space.

By default, thin provisioning is disabled for existing file systems and for newly created file systems. Enable and disable thin provisioning using the `filesystem-thin` command (currently there is no way to enable or disable thin provisioning through the Web Manager GUI).
Thin provisioning works on a per file system basis, and does not affect the capacity reported by the `span-list --filesystems` and `filesystem-list` commands. Also, Web Manager (the GUI) displays the actual file system size. As a result, the administrator can perform proper capacity planning.

When enabled, thin provisioning information is returned by the following CLI commands:

- `cifs-share list`
- `df`
- `filesystem-limits`
- `filesystem-list -v`
- `fs-stat`
- `nfs-export list`
- `query`

For more information about CLI commands, refer to the *Command Line Reference*.

If thin provisioning is enabled and you disable file system auto-expansion for a storage pool, the free space reported for each of the file systems in that storage pool is the same as if thin provisioning were not enabled. This means that the free space reported becomes equal to the difference between the file system’s current usage and the amount of space in all storage pool chunks currently allocated to that file system. If you re-enable file system auto-expansion for file systems in the storage pool, free space is again reported as the difference between the file system’s current usage and its expansion limit, if an expansion limit has been specified.

When thin provisioning is enabled, and the aggregated file system expansion limits of all file systems exceeds the amount of storage connected to the server/cluster, warnings are issued to indicate that storage is oversubscribed. These warnings are issued because there is an insufficient amount of actual storage space for all file systems to grow to their expansion limit.

### Managing file system expansion

File system growth management strategies can be summarized as follows:

- **Auto-expansion enabled, but not confined.** The file system is created with a defined size limit, and a small amount of that space is actually allocated when the file system is created. The file system is then allowed to expand automatically (auto-expansion enabled) until the storage pool hosting the file system is full (auto-expansion is not confined), as long as the file system expansion will not cause the file system to exceed the maximum allowable number of chunks in a file system.

- **Auto-expansion enabled, and confined.** The file system is created with a defined size limit, and a small amount of that space is actually allocated when the file system is created. The file system is then allowed to expand automatically (auto-expansion enabled) to the defined size limit (auto-
expansion is confined), as long as there is available space in the storage pool and the file system expansion will not cause the file system to exceed the maximum allowable number of chunks in a file system.

- **Auto-expansion disabled.** The file system is created with the full amount of the specified size, and is not allowed to expand automatically (auto-expansion disabled).

**Note:** The size of a file system cannot be reduced.

<table>
<thead>
<tr>
<th>File System Type</th>
<th>Auto-Expansion Enabled</th>
<th>Auto-Expansion Disabled</th>
</tr>
</thead>
</table>
| Untiered         | **If auto-expansion is not confined,** the size limit is ignored. The file system will be allowed to expand until the storage pool is full.  
**If auto-expansion is confined,** the size limit defines the maximum size to which a file system will be allowed to expand.  
When the file system is created, it is initially allocated a certain amount of space (the initial capacity), and the file system is allowed to expand automatically, up to its size limit. When the file system uses approximately 80% of its currently allocated space, it is expanded automatically up to its size limit. This expansion occurs in increments specified by the guideline chunk size (which is calculated by the system).  
The file system can be manually expanded, increasing the file system size limit. | The size limit defines the amount of space that is immediately allocated to the file system.  
When the file system is created, it is allocated the total amount of space specified by the size limit.  
The file system can be manually expanded, increasing the file system size limit. |
| Tiered           | **If auto-expansion is not confined,** the size limit is ignored if defined. The tiers of the file system will be allowed to expand until the storage pool is full.  
**If auto-expansion is confined,** the size limit defines the maximum size to which the tier of a file system will be allowed to expand.  
When the file system is created, the user data tier is initially allocated a certain amount of space (the initial capacity), and the user data tier is allowed to expand automatically, up to its size limit. When the user data tier uses approximately 80% of its currently allocated space, it is expanded automatically up to its size limit. This expansion occurs in increments specified by the guideline chunk size (which is calculated by the system).  
Either tier can be manually expanded, increasing the file system size limit. | The size limit defines the amount of space that is immediately allocated to the user-data tier.  
When the file system is created, the user data tier is initially allocated the total amount of space specified by the size limit.  
Either tier can be manually expanded, increasing the file system size limit. |
When the file system is created, the user data tier is initially allocated the total amount of space specified by the size limit. Either tier can be manually expanded, increasing the file system size limit.

By default, file system auto-expansion is enabled and, when auto-expansion is enabled, the file system expands, without interruption of service if the following conditions exist:

- **Confined limit not reached** (only for file systems that have auto-expansion confined). As long as the file system expansion would not exceed the confined auto-expansion limit.
- **Available space**. Sufficient available free space and chunks remain in the storage pool.
- Chunk limit. The file system expansion will not cause the file system to exceed the maximum allowable number of chunks in a file system.
- **Maximum supported file system size**. The file system expansion will not cause the file system to exceed the maximum supported file system size.

Whether auto-expansion is enabled or disabled, you can limit the size of the file system of an untiered file system or either tier of a tiered file system. If necessary, you can manually expand the file system or of an untiered file system or a tier of a tiered file system.

Note: File system auto-expansion may be enabled or disabled for all file systems in a particular storage pool. When enabled for a storage pool, file system auto-expansion is enabled by default, but if it has been disabled on an individual file system, you can re-enable it. When file system auto-expansion is disabled for a storage pool, you cannot enable it (you must expand the file system manually).

### Enabling and disabling file system auto-expansion

When file system auto-expansion is enabled or disabled for a storage pool, you cannot change the setting for a single file system in the storage pool; you must enable or disable file system auto-expansion for all file systems in the storage pool.

When file system auto-expansion is disabled and a file system requires expansion, you must expand the file system manually.

The ability for file systems in a storage pool to automatically expand is enabled or disabled at the storage pool level.
• When file system auto-expansion is enabled for a storage pool, file systems in the storage pool may be allowed to auto-expand or they may be confined to a specified size limit. File system auto-expansion is enabled or disabled for each file system independently.

• When file system auto-expansion is disabled for a storage pool, file systems in the storage pool are not allowed to auto-expand. You cannot change the setting for an individual file system in the storage pool to allow auto-expansion.

When file system auto-expansion is disabled (at the storage pool level, or for an individual file system) and a file system requires expansion, you must expand the file system manually.

Confining file system auto-expansion
Instructions on how to confine the maximum size of a file system.

To confine (limit) the maximum size of an untiered file system or the user data tier of a tiered file system:

Procedure
1. From the Home page, navigate to Storage Management > File Systems to display the File System page.
2. Select a file system and click details to display the File System Details page.
3. To define auto-expansion confinement settings, choose from one of the following choices:
   • If a tiered file system must not expand beyond a specific size, enter the size limit in the Confine Auto-Expansion field.
   • If an untiered file system must not expand beyond a specific size, enter the size limit in the Confine Auto-Expansion field.
4. Click Apply.

Unconfining file system auto-expansion
To unconfine (remove the limit on) the maximum size of an untiered file system or a tier of a tiered file system:

Procedure
2. Select a file system and click details to display the File System Details page.
3. To remove auto-expansion confinement settings, choose from one of the following choices:
   • If a tiered file system must not be limited to a specific size, delete the current size limit in the Confine Auto-Expansion field.
• If an untiered file system must not be limited to a specific size, delete the current size limit in the **Confine Auto-Expansion** field.

4. Click **Apply**.

**Expanding file system manually**

Manual file system expansion is supported through the Web Manager and through the CLI.

**Procedure**

1. Navigate to **Home > Storage Management > File Systems**.
2. Select a file system and click **details** to display the **File System Details** page.
3. Click **expand** to display the **Expand File System** page.

For an untiered file system the **Expand File System** page looks like the following:

![Expand File System Page](image1)

For a tiered file system, the **Expand File System** page looks like the following:

![Expand File System Page](image2)
4. To expand the file system manually, do one of the following:
   - For an untiered file system, specify the new file system capacity in the **New Capacity** field and use the list to select MB, GB, or TB.
   - For a tiered file system, select the tier you want to expand, and specify the new file system capacity in the **New Capacity** field, then use the list to select MB, GB, or TB.

**Note:** You can expand one tier per expansion operation. To expand both tiers, you must perform a manual expansion twice.

5. Click **OK**.

**Note:** Because space is always allocated in multiples of the chunk size set when the storage pool containing the file system was created, the final size of the file system may be slightly larger than you request.

Manual expansion of file systems is also supported through the command line interface. For detailed information on this process, run `man filesystem-expand` on the CLI.

**Virtual volumes**

A file system can be divided into discrete areas of storage called virtual volumes. From a client’s perspective, a virtual volume appears to be a normal file system. A virtual volume provides a simple method for allocating and controlling directories for projects, users, or groups. Capacity and number of files within a virtual volume can be controlled using quotas.

The terms user and group are used to indicate NFS or CIFS users and groups.

Virtual volumes have the following characteristics:
- **Name**: A name or label by which the virtual volume is identified. This will often be the same as a CIFS share or NFS export rooted at the volume’s root directory.
- **File System**: The file system in which the virtual volume is created.
- **Path**: The directory at the root of the virtual volume.
- **Email Contacts**: A list of email addresses, to which information and alerts about virtual volume activity are sent. The list can also be used to send emails to individual users.
- **Moving Files**: You can move files in or out of a virtual volume.
- **Moving Directories**: Moving a directory in or out of a virtual volume will return a cross volume link error. However, most CIFS or NFS clients will suppress this error and, instead, will copy the directory to the target location and then delete the original directory.
- **Linking Files** (hard links): You cannot link files across different virtual volumes.
**Important information about virtual volumes and quotas**

The server treats the virtual volume ‘root’ directory, together with all its sub-directories, as a self-contained file system. The virtual volume tracks its usage of space and number of files, to provide a way of monitoring file system usage. This tracking allows quotas to be imposed on disk space usage, as well as the total number of files.

Quotas can be set for the entire virtual volume, and on individual users, and on groups of users. Default user and group quotas can be defined, and in the absence of explicit user or group quotas, the default quotas apply.

The following caveats apply in measuring the virtual volume status against quota thresholds:

- **Metadata and snapshot files.** Neither file system metadata nor snapshot files count towards the quota limits.

- **Symbolic link calculation.** Files with multiple hard links pointing to them are included only once in the quota calculation. A symbolic link adds the size of the symbolic link file to a virtual volume and not the size of the file to which it links.

**Managing usage quotas**

The **Quotas by File System** page lists usage quotas for the selected file system.
Procedure

1. Navigate to **Home > Storage Management > Quotas by File System** to display the **Quotas by File System** page.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS/File System</td>
<td>The name of the selected EVS and file system.</td>
</tr>
<tr>
<td><strong>change</strong></td>
<td>Use to select a different file system to display a different set of quotas.</td>
</tr>
<tr>
<td>Filter</td>
<td>Use to reduce the number of quotas or virtual volumes displayed on the page.</td>
</tr>
<tr>
<td>User/Group Account</td>
<td>A quota name can consist of:</td>
</tr>
<tr>
<td></td>
<td>• A CIFS domain and user or group name, such as bb\Smith or bb\my_group</td>
</tr>
<tr>
<td></td>
<td>(where bb is a domain, Smith is a user and my_group is a group).</td>
</tr>
<tr>
<td></td>
<td>• An NFS user or group such as richardb or finance (where richardb is an</td>
</tr>
<tr>
<td></td>
<td>NFS user and finance is an NFS group).</td>
</tr>
<tr>
<td></td>
<td>A name may be '0' (if the quota was created for the owner of the directory</td>
</tr>
<tr>
<td></td>
<td>at the root of the virtual volume).</td>
</tr>
<tr>
<td>File systems</td>
<td>The file system on which the quota applies.</td>
</tr>
<tr>
<td>Quota Type</td>
<td>Type of file system activity. Possible values are User, Group, or Virtual</td>
</tr>
<tr>
<td></td>
<td>Volume. The value virtual volume applies to anyone initiating activity</td>
</tr>
<tr>
<td></td>
<td>in the entire virtual volume, and only one quota with this target type</td>
</tr>
<tr>
<td></td>
<td>can exist on each virtual volume.</td>
</tr>
<tr>
<td>Created By</td>
<td>Lists the method of quota creation:</td>
</tr>
<tr>
<td></td>
<td>• Automatically Created: A quota created using a quota default.</td>
</tr>
<tr>
<td></td>
<td>• User Defined: A uniquely defined quota.</td>
</tr>
<tr>
<td>Usage Limit</td>
<td>Overall limit set for the total size of all files in the file system</td>
</tr>
<tr>
<td></td>
<td>owned by the target of the quota.</td>
</tr>
</tbody>
</table>
### Field/Item Description

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Count Limit</td>
<td>Overall limit set for the total number of files in the file system owned by the target of the quota.</td>
</tr>
<tr>
<td>details</td>
<td>Displays the <a href="#">File System Quotas Details</a> page for the selected file system.</td>
</tr>
<tr>
<td>add</td>
<td>Advances to the <a href="#">Add File System Quota</a> page.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes a particular quota.</td>
</tr>
<tr>
<td>Delete All Quotas</td>
<td>Deletes all of the current quotas for the virtual volume.</td>
</tr>
<tr>
<td>Refresh cache</td>
<td>Clears the SMU's cache and repopulates it with relevant objects. (This is different than clicking the browser refresh button, which picks up any recent updates without clearing the cache.)</td>
</tr>
<tr>
<td>User Defaults</td>
<td>Use to set, edit, or reset the user defaults.</td>
</tr>
<tr>
<td>Group Defaults</td>
<td>Use to set, edit, or reset the group defaults.</td>
</tr>
<tr>
<td>Modify Email</td>
<td>Use to edit the list of contacts who are notified when quotas are reached.</td>
</tr>
<tr>
<td>Contacts</td>
<td></td>
</tr>
<tr>
<td>Download Quotas</td>
<td>Use to download the quotas (not file system quotas) for this virtual volume to a <code>.csv</code> file.</td>
</tr>
</tbody>
</table>

### Setting user and group file system quota defaults

The quota default values define a template with which the system will automatically generate a quota in response to a file being saved on the file system. If a file is saved, and the respective defaults are set, a user quota will be created for the user, and a group quota created for the user's domain. In addition, as soon as the defaults are set, a user and group quota will be created for the owner of the directory at the root of the virtual volume.

**Procedure**

1. Navigate to [Home > Storage Management > Quotas by File System](#) to display the [Quotas by File System](#) page.
2. In the **Quotas by File System** page, click User Defaults or Group Defaults. User Defaults creates a user quota for the user; a Group quota creates a group quota for the user's domain.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS/File System</td>
<td>The EVS and file system on which the user file system quota applies.</td>
</tr>
<tr>
<td><strong>change</strong></td>
<td>Use to select another EVS or file system.</td>
</tr>
<tr>
<td>Automatically create quotas</td>
<td></td>
</tr>
<tr>
<td>for Domain Users</td>
<td></td>
</tr>
<tr>
<td></td>
<td><img src="https://www.example.com" alt="Note: This option only displays in the Group File System Quota Defaults" /> page.</td>
</tr>
<tr>
<td></td>
<td>This option allows the creation of default quotas for the group</td>
</tr>
<tr>
<td></td>
<td>Domain Users. By default every NT user belongs to the group</td>
</tr>
<tr>
<td></td>
<td>Domain Users. Enabling this option effectively includes every NT user in the</td>
</tr>
<tr>
<td></td>
<td>quota, (unless each user's primary group has been explicitly set).</td>
</tr>
<tr>
<td><strong>Usage</strong></td>
<td></td>
</tr>
<tr>
<td>Limit</td>
<td>Amount of space to enable in Bytes: KB, MB, GB or TB.</td>
</tr>
<tr>
<td>Hard Limit</td>
<td>When enabled, the amount of space specified in the Limit field cannot be</td>
</tr>
<tr>
<td></td>
<td>exceeded.</td>
</tr>
<tr>
<td>Warning</td>
<td>Percentage of the amount of space specified in the Limit field at which a</td>
</tr>
<tr>
<td></td>
<td>Warning alert will be sent.</td>
</tr>
<tr>
<td>Severe</td>
<td>Percentage of the amount of space specified in the Limit field at which a</td>
</tr>
<tr>
<td></td>
<td>Severe alert will be sent.</td>
</tr>
<tr>
<td><strong>File Count</strong></td>
<td></td>
</tr>
<tr>
<td>Limit</td>
<td>Maximum number of files to enable for this quota.</td>
</tr>
<tr>
<td>Field/Item</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Hard Limit</td>
<td>When enabled, the number of files specified in the Limit field cannot be exceeded.</td>
</tr>
<tr>
<td>Warning</td>
<td>The percentage of the number of files specified in the Limit field at which a Warning alert will be sent.</td>
</tr>
<tr>
<td>Severe</td>
<td>Percentage of the amount of space specified in the Limit field at which a Severe alert will be sent.</td>
</tr>
<tr>
<td>Log Quota Events in the managed server's Event log</td>
<td>Filling this check box sets the default for all users or groups to have quota events logged in the server’s event log.</td>
</tr>
<tr>
<td>OK</td>
<td>Saves configuration changes, and closes the page.</td>
</tr>
<tr>
<td>clear defaults</td>
<td>Reset all the defaults to zero and any existing quotas generated automatically will be converted into user defined quotas.</td>
</tr>
<tr>
<td>cancel</td>
<td>Closes the page without saving configuration changes.</td>
</tr>
</tbody>
</table>

3. For group file system quota defaults, fill in the **Automatically create quotas for Domain Users** check box to allow the creation of default quotas for the group domain users.

4. Under the Usage and File Count sections, enter the values as appropriate:
   a. In the **Limit** field, enter the limit. In the Usage section, additionally, select KB, MB, GB, or TB from the list.
   b. Fill in the **Hard Limit** check box if the space specified in the Limit field cannot be exceeded.
   c. In the **Warning** field, enter the warning.
   d. In the **Severe** field, enter the value.
   e. Fill in the **Log Quota Events in the managed server's EventLog** check box to set the default for all users or groups to have quota events logged in the server’s event log.

5. Click **OK**.

**Adding a quota**

Describes how to allocate storage usage and file count by client.

**Procedure**

1. Navigate to **Home > Storage Management > Quotas by File System** to display the **Quotas by File System** page.
2. Click **add** in the **Add File System Quota** page.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS/File System</td>
<td>The EVS and file system on which the user file system quota applies.</td>
</tr>
<tr>
<td><strong>change</strong></td>
<td>Use to select another EVS or file system.</td>
</tr>
<tr>
<td>Quota Type</td>
<td>Type of source of virtual volume activity. Possible values are User, Group, or Virtual Volume. Virtual Volume applies to anyone initiating activity in the entire virtual volume, and only one quota with this target type can exist on each virtual volume.</td>
</tr>
<tr>
<td><strong>Usage</strong></td>
<td></td>
</tr>
<tr>
<td>Limit</td>
<td>Amount of space to enable in Bytes: KB, MB, GB or TB.</td>
</tr>
<tr>
<td>Hard Limit</td>
<td>When enabled, the amount of space specified in the Limit field cannot be exceeded.</td>
</tr>
<tr>
<td>Warning</td>
<td>Percentage of the amount of space specified in the Limit field at which a Warning alert will be sent.</td>
</tr>
<tr>
<td>Severe</td>
<td>Percentage of the amount of space specified in the Limit field at which a Severe alert will be sent.</td>
</tr>
<tr>
<td><strong>File Count</strong></td>
<td></td>
</tr>
<tr>
<td>Limit</td>
<td>Maximum number of files to enable for this quota.</td>
</tr>
<tr>
<td>Hard Limit</td>
<td>When enabled, the number of files specified in the Limit field cannot be exceeded.</td>
</tr>
<tr>
<td>Warning</td>
<td>The percentage of the number of files specified in the Limit field at which a Warning alert will be sent.</td>
</tr>
</tbody>
</table>

Managing file system performance

Hitachi NAS Platform File Services Administration Guide
3. Click **User** to add a user account, or **Group** to add a group account. If the Quota Type is Virtual Volume, a name is not required. The name may consist of both a domain (maximum 16 characters) and a user or group name (maximum 256 characters), such as `my_domain\my_name`, but may not include a colon (`:`).

4. Under the Usage and File Count sections, enter the values as appropriate:
   a. In the **Limit** field, enter the limit. In the Usage section, additionally, select KB, MB, GB, or TB from the list.
   b. Fill in the **Hard Limit** check box if the space specified in the Limit field cannot be exceeded.
   c. In the **Warning** field, enter the warning.
   d. In the **Severe** field, enter the value.
   e. Fill in the **Log Quota Events in the managed server's Event Log** check box to set the default for all users or groups to have quota events logged in the server’s event log.

5. Click **OK**.

**Modifying a file system quota**

**Procedure**

1. Navigate to **Home > Storage Management > Quotas by File System** to display the **Quotas by File System** page.
2. Fill in the check box next to the quota, and click **details**.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS/File System</td>
<td>The EVS and file system on which the user file system quota applies.</td>
</tr>
<tr>
<td>change</td>
<td>Use to select another EVS or file system.</td>
</tr>
<tr>
<td>Quota Type</td>
<td>Type of source of virtual volume activity. Possible values are User, Group, or Virtual Volume. Virtual Volume applies to</td>
</tr>
</tbody>
</table>
anyone initiating activity in the entire virtual volume, and only one quota with this target type can exist on each virtual volume.

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Usage</strong></td>
<td></td>
</tr>
<tr>
<td>Limit</td>
<td>Amount of space to enable in Bytes: KB, MB, GB or TB.</td>
</tr>
<tr>
<td>Hard Limit</td>
<td>When enabled, the amount of space specified in the Limit field cannot be exceeded.</td>
</tr>
<tr>
<td>Warning</td>
<td>Percentage of the amount of space specified in the Limit field at which a Warning alert will be sent.</td>
</tr>
<tr>
<td>Severe</td>
<td>Percentage of the amount of space specified in the Limit field at which a Severe alert will be sent.</td>
</tr>
<tr>
<td><strong>File Count</strong></td>
<td></td>
</tr>
<tr>
<td>Limit</td>
<td>Maximum number of files to enable for this quota.</td>
</tr>
<tr>
<td>Hard Limit</td>
<td>When enabled, the number of files specified in the Limit field cannot be exceeded.</td>
</tr>
<tr>
<td>Warning</td>
<td>The percentage of the number of files specified in the Limit field at which a Warning alert will be sent.</td>
</tr>
<tr>
<td>Severe</td>
<td>Percentage of the amount of space specified in the Limit field at which a Severe alert will be sent.</td>
</tr>
<tr>
<td><strong>Log Quota Events in the managed server's Event log</strong></td>
<td>Filling this check box sets the default for all users or groups to have quota events logged in the server’s event log.</td>
</tr>
<tr>
<td><strong>OK</strong></td>
<td>Saves configuration changes, and closes the page.</td>
</tr>
<tr>
<td><strong>cancel</strong></td>
<td>Closes the page without saving configuration changes.</td>
</tr>
</tbody>
</table>

3. Make any necessary changes, and click **OK**.

**Deleting a file system quota**

**Procedure**

1. Navigate to **Home > Storage Management > Quotas by File System** to display the **Quotas by File System** page.
2. Fill in the check box next to one or more quotas and then click **delete**.

**Moving a file system**

Moving a file system (or several file systems) may be necessary to improve performance or balance loads, to move data to different storage resources, to support changing network topography, or other reasons.

There are two basic methods of moving a file system:
• File System Relocation

File system relocation changes the EVS (virtual server) that hosts the file system, but it does not move file system data. Moving the file system from one EVS to another changes the IP address used to access the file system, and also changes CIFS shares and NFS Exports for that file system. For information on how to relocate a file system using File System Relocation, refer to the *Replication and Disaster Recovery Administration Guide*.

If the file system to be relocated is linked to from within a CNS, and clients access the CNS using a CIFS share or an NFS export, the relocation can be performed with no change to the configuration of network clients. In this case, clients will be able to access the file system through the same IP address and CIFS share/NFS export name after the relocation as they did before the relocation was initiated. For more information on CNS, refer to the *Server and Cluster Administration Guide*.

**Caution:** Whether or not the file system resides in a CNS, relocating a file system will disrupt CIFS communication with the server. If Windows clients require access to the file system, the file system relocation should be scheduled for a time when CIFS access can be interrupted.

• Transfer of primary access

A transfer of primary access is a replication-based method of copying data from a portion of a file system (or an entire file system) and relocating the access points for that data (copying the data and metadata). A transfer of primary access causes very little down time, and the file system is live and servicing file read requests during most of the relocation process. For a short period during the relocation process, access is limited to read-only. For more information on relocating a file system using transfer of primary access, refer to the *Replication and Disaster Recovery Administration Guide*.

The method you use to relocate a file system depends, in part, on what you want to move, and what you want to accomplish by relocating the file system.

• If you want to move the file system’s access points, but not the actual data, using file system relocation is the most appropriate method.

• If you want to move the file system’s data and access points, using a transfer of primary access is the most appropriate method.

**File system relocation**

Before it can be shared or exported, a file system must be associated with a Virtual Server (EVS), thereby making it available to network clients. The association between a file system and an EVS is established when the file system is created. Over time, evolving patterns of use and/or requirements for storage resources may make it desirable to relocate a file system to a different EVS.
Note: Read caches cannot be relocated.

A file system hosted by an EVS on a cluster node may be relocated to:
- An EVS on the same cluster node, or
- An EVS on a different node in the same cluster.
  but may not be relocated to:
- An EVS on a stand-alone server, or
- An EVS on a node of a different cluster.

A file system hosted by an EVS on a stand-alone server may be relocated to
- An EVS on the same server
  but may not be relocated to:
- An EVS on a different server, or
- An EVS on a node in a cluster.

Typically, File System Relocation is used to move a file system from an EVS on a cluster node to an EVS on a different cluster node in order to improve throughput by balancing the load between cluster nodes.

File system relocation performs the following operations:
- Re-associates the file system with the selected EVS.
- Transfers explicit CIFS shares of the file system to the new EVS.
- Transfers explicit NFS exports of the file system to the new EVS.
- Migrates FTP users to the new EVS.
- Migrates snapshot rules associated with the file system to the new EVS.
- Migrates the iSCSI LUs and targets.

File system relocation may require relocating more than just the specified file system. If the file system is a member of a data migration path, both the data migration source file system and the target file system will be relocated. It is possible for the target of a data migration path to be the target for more than one source file system. If a data migration target is relocated, all associated source file systems will be relocated as well.

If more than one file system must be relocated, a confirmation dialog will appear indicating the additional file systems that must be moved. Explicit confirmation must be acknowledged before the relocation will be performed.

File System Relocation will affect the way in which network clients access the file system in any of the following situations:
- The file system is linked to from the CNS tree, but is shared or exported outside of the context of the CNS.
- The cluster does not use a CNS.

In each of the above cases, access to the shares and exports will be changed. In order to access the shares and exports after the relocation, use an IP address of the new EVS to access the file service.
Relocating file systems that contain iSCSI Logical Units (LUs) will interrupt service to attached initiators, and manual reconfiguration of the IP addresses through which targets are accessed will be required once the relocation is complete. If relocating a file system with LUs is required, the following steps must be performed:

- Disconnect any iSCSI Initiators with connections to LUs on the file system to be relocated.
- Unmount the iSCSI LU.
- Relocate the file system as normal. This procedure is described in detail in the *Replication and Disaster Recovery Administration Guide*.
- Reconnect the new Targets with the iSCSI Initiators. Be aware that the Targets will be referenced by a new name corresponding to the new EVSs.

**Note:** All iSCSI LUs on a target must be associated with file systems hosted by the same EVS.

**Using system lock on file systems**

System Lock mode protects file systems during replication and transfer of primary access operations. Four important distinctions apply:

- **NDMP (Network Data Management Protocol) versus file service protocols.** When System Lock is enabled for a file system:
  - NDMP has full access (including writes) during backups, replication, and transfer of primary access.
  - The file system remains in read-only mode to clients using the file service protocols (NFS, CIFS, FTP, and iSCSI).

- **System Lock versus read only:**
  - When a file system is Syslocked, NDMP still has full access to that file system and can write to it.
  - When a file system is mounted as read-only, NDMP (like all other protocols) has read-only access to that file system, and cannot write to it. To ensure that a file system remains completely unchanged, you should mount it as read-only.

- **Replication versus transfer of primary access:**
  - During replication operations, the destination file system is put into System Lock mode.
  - During transfer of primary access operations, both the source file system and the destination file system are put into System Lock mode.

- **Read Cache Exception.** A read cache may not be put into System Lock mode.

**Enabling and disabling system lock for a file system**

**Procedure**

1. Navigate to **Home > Storage Management > File Systems.**
2. Select a file system and click **details** to display the **File System Details** page.

3. In the **Syslock** field, toggle the enable/disable button as appropriate.

   When the file system is in System Lock mode, the Status changes to Syslocked, the System Lock status becomes enabled, and the **Enable** button becomes **Disable**.

   When System Lock is enabled for a file system, NDMP has full access to the file system and can write to it during a backup or replication, but the file system remains in read-only mode to clients using the file service protocols (NFS, CIFS, FTP, and iSCSI).

   When viewing the details of a read cache, the System Lock’s enable/disable button is not available.

**Recovering a file system**

Following some system failures, a file system may require recovery before mounting. If required, such a recovery is performed automatically when you mount the file system. Performing recovery rolls the file system back to its last checkpoint and replays any data in NVRAM.

In extreme cases, when you mount a file system after a system failure, the automatic recovery procedures may not be sufficient to restore the file system to a mountable condition. In such a case, you must forcefully mount the file system, which discards the contents of NVRAM before mounting the file system.

**Procedure**

1. Navigate to **Home > Storage Management > File Systems**.
2. Select a file system and click **details** to display the **File System Details** page.
3. If a file system displays Not Mounted in the Status column, click **mount** to try to mount the file system.
   - If necessary, the automatic recovery processes will be invoked automatically. The file system was mounted successfully.
   - If the automatic recovery fails, the file system will not mount, and the **File Systems** page will reappear, indicating that the file system was not mounted. Navigate to the **File System Details** page. Continue with **Recovering a file system on page 67**.
4. For the file system that failed to mount, click **details** to display the **File System Details** page. In the Settings/Status area of the page, the file system label will be displayed, along with the reason the file system failed to mount (if known), and suggested methods to recover the file system, including the link for the **Forcefully mount** option.
5. Depending on the configuration of your system, and the reason the file system failed to mount, you may have several recovery options:

- *If the server is part of a cluster*, you may be able to migrate the assigned EVS to another cluster node, then try to mount the file system. This can become necessary when another node in the cluster has the current available data in NVRAM that is necessary to replay write transactions to the file system following the last checkpoint. An EVS should be migrated to the cluster node that mirrors the failed node’s NVRAM (for more information on NVRAM mirroring, refer to the *System Access Guide*. For more details on migrating EVSs, refer to the *Server and Cluster Administration Guide*.

- *If the first recovery attempt fails*, click the **Forcefully mount** link. This will execute a file system recovery without replaying the contents of NVRAM.

**Caution:** Using the Forcefully mount option discards the contents of NVRAM, data which may have already been acknowledged to the client. Discarding the NVRAM contents means that all write operations in NVRAM (those write operations not yet committed to disk) are lost. The client will then have to resubmit the write request. Use the Forcefully mount option only upon the recommendation of Hitachi Data Systems Support Center.

### Restoring a file system from a checkpoint (WFS-2 only)

Following a storage subsystem failure, it may be necessary to recover file systems. WFS-2 file systems have better file system resiliency following storage subsystem failures than WFS-1 file systems. File systems formatted using WFS-2 have underlying redundant metadata structures, which allow them to be recovered from checkpoints or snapshots. File systems formatted using WFS-1 do not have the same underlying redundant metadata structures, and so cannot be recovered from checkpoints or snapshots.

File system corruption due to an event (such as RAID controller crash, storage system component failure, or power loss) often affects objects that were being modified around the time of the event.

WFS-2 preserves multiple checkpoints for a file system. By default, a WFS-2 file system is configured to keep up to 128 checkpoints. The maximum number of checkpoints supported is 1024. The number of checkpoints preserved is configurable when the file system is formatted, but, once set, the number of checkpoints cannot be changed.

When a checkpoint completes, rather than immediately freeing the storage used for the previous checkpoint, WFS-2 maintains a number of old checkpoints. As each new checkpoint completes, the oldest checkpoint is overwritten. This means that there can be multiple checkpoints on-disk, each of which is complete and internally consistent point-in-time view of the file.
system. If necessary, the file system can be restored to any of these checkpoints.

In the case of file system corruption, if there are enough checkpoints on disk, it may be possible to roll back to a previous checkpoint, pre-dating the event that caused the corruption and restoring the file system using the uncorrupted checkpoint. This may be possible even if this event occurred up to a few minutes before the file system was taken offline.

To restore a file system to a previous checkpoint, use the `fs-checkpoint-health` and the `fs-checkpoint-select` commands. Refer to the Command Line Reference for more information about these commands.

Note the following:

- Restoring a file system using a checkpoint does not affect snapshots taken prior to the checkpoint being restored, but, like any other file system update, snapshots taken after that checkpoint are lost.
- After restoring to a checkpoint, it is possible to restore again, to an older checkpoint and, if the file system has not been modified, restore again, to a more recent checkpoint. So, for example, it is possible to mount the file system in read only mode, check its status, and then decide whether to remount the file system in normal (read/write) mode or to restore to a different checkpoint.

**Caution:** Once you mount a restored file system in normal (read/write) mode, you cannot restore to a later checkpoint.

**File system recovery from a snapshot (WFS-2 only)**

It is possible that, although corruption has occurred in the live file system, a good snapshot still exists. If so, it may be preferable to recover the file system from this snapshot, with some loss of data, rather than incur the downtime that might be required to fix the live file system. Recovering a file system from a snapshot restores the file system to the state that it was in when the snapshot was taken.

Recovering a file system from a snapshot makes it possible to roll back the file system to the state that it was in when a previous snapshot was taken.

File system recovery from a snapshot is a licensed feature, which requires a valid FSRS license on the server/cluster.

**Note:** You can recover a file system from a snapshot only when at least the configured number of preserved file system checkpoints have been taken since that snapshot was taken. For example, if a file system is configured to preserve 128 checkpoints (the default), then you can recover the file system from a snapshot only after a minimum of 128 checkpoints have been taken after the snapshot. If less than the configured number of checkpoints have
been taken since the snapshot, you can either recover from an earlier snapshot or recover the file system from a checkpoint.

Note:

The following file system rollback considerations apply:

- File system rollback can be performed even if the live file system is corrupted.
- All snapshots are lost after the rollback.
- Even though the file system recovery happens very quickly, no new snapshots can be taken until all previous snapshots have been discarded. The time required before a new snapshot can be taken depends on the size of the file system, not on the number of files in the file system.

Note: Once you have recovered a file system from a snapshot, and mounted it in read-write mode, you cannot undo the recovery or recover again to a different snapshot or checkpoint.

To roll back a file system from a snapshot, use the `snapshot-recover-fs` command. Refer to the Command Line Reference for more information about this command.

**Automatic file system recovery (WFS-1 and WFS-2)**

The command line interface for file system recovery accommodates WFS-2 file systems. The `fixfs` utility is the main file system recovery tool for WFS-1 and WFS-2 file systems, but it should only be used under the supervision of Hitachi Data Systems Support Center personnel. An additional tool is available to kill all current snapshots, that is the `kill-snapshots` command (refer to the Command Line Reference for more information about this command).

`fixfs` is capable of repairing a certain amount of non-critical metadata, for example performing orphan recovery. At all stages that have the potential to last longer than a few minutes, `fixfs` provides progress reporting, and the option to abort the fix. Note that progress reports are stage or operation based, for example Stage 3 of 7 complete. For some operations, `fixfs` will also provide an estimate of time until the completion of the operation.

The strategy used by `fixfs` to repair file systems can be summarized as:

- `fixfs` is the only recovery tool to be used if a file system is experiencing corruption. The default `fixfs` behavior may be modified by various command line switches, but often the required switch is suggested by `fixfs` during or at the end of a previous run.
- Where possible, `fixfs` will run with the file system in any state (there will be no need to perform file system recovery first, so that there’s no need to worry about what happens if recovery cannot complete due to corruption). Where not possible (for example, if the file system is already mounted, or
is marked as "failed" or "requires expansion"), **fixfs** will not run. When **fixfs** does not run, it will give a clear indication of what needs to be done to get to the point where it can run.

- By default, **fixfs** will only modify those objects which are lost or corrupted.
- By default, **fixfs** will only bring the file system to the point where it can be mounted.
- Snapshots are considered expendable and are deleted.

**Using deduplication file system**

This section describes how to use deduplication on a file system.

- You can configure a new file system to support and enable dedupe.
- An existing WFS-2 file system can be converted to be dedupe-enabled.
- File systems with support for dedupe can be dedupe-enabled or dedupe-disabled.

**Determining sufficient space for dedupe conversion**

Non-dedupe enabled file systems must be converted before they will support deduplication. However, the conversion process is an offline process which can sometimes fail because there is not sufficient scratch or free space available. In this scenario, you must expand the file system and then re-attempt the conversion.

Before you start the dedupe conversion, use the following procedure to determine if a file system has sufficient scratch and free space available. It is not an offline procedure.

**Procedure**

1. Call Hitachi Data Systems Support Center to obtain the instructions and dev password to execute the **fs-capacity-info** dev command.
   This command can be run on a mounted file system.
2. Run the command with the name of the file system that is to be checked (for example, **fs-capacity-info -f filesystem1**).
   This command generates the following sample output:

   ```
   fs-capacity-info/fs3: Underlying length : 0x017666400000 bytes, 0x00bb332000 sectors, 0x017666400 blocks
   fs-capacity-info/fs3: Formatted length : 0x017636000000 bytes, 0x00bb1b0000 sectors, 0x017636000 blocks
   fs-capacity-info/fs3: Scratch-space offset : 0x017636000000 bytes, 0x00bb1b0000 sectors, 0x017636000 blocks
   fs-capacity-info/fs3: Scratch-space length : 0x000030400000 bytes, 0x0000182000 sectors, 0x000030400 blocks
   fs-capacity-info/fs3: Reservable available space : 0x01748e51f000 bytes, 0x00ba4728f8 sectors, 0x01748e51f blocks
   fs-capacity-info/fs3: Physical available space : 0x0175ff4bb000 bytes, 0x00baffa5d8 sectors, 0x0175ff4bb
   ```
blocks
fs-capacity-info/fs3: Space required for RCB conversion:
0x0000e9e1c000 bytes, 0x000074f0e0 sectors, 0x0000e9e1c blocks
fs-capacity-info/fs3: Scratch-space required for RCB conversion:
0x00002eccc800 bytes, 0x0000176664 sectors, 0x00002eccc blocks

3. Locate the “Scratch-space length” value. In this example, 0x000030400000 bytes.

4. Locate the “Scratch-space required for RCB conversion” value. In this example, 0x00002eccc800 bytes.

5. If the Scratch-space length is greater than Scratch-space required for RCB conversion, then there is enough scratch space. In this example, 0x000030400000 is greater than 0x00002eccc800, indicating that there is enough scratch space for the conversion.

6. Locate the “Reservable available space” value. In this example, 0x01748e51f000 bytes.

7. Multiply the Space required for RCB conversion value by 1.6. In this example, the value is 0x000176360000 bytes.

8. If Reservable available space is greater than Space required for RCB conversion * 1.6, then there is enough free space. 0x01748e51f000 is greater than 0x000176360000, indicating there is enough free space for the conversion.

Preparing for dedupe conversion

In addition to the space required for the ondisk component (for example, 45 GB) of the dedupe index, a conversion process may also require additional scratch space that is normally carved out of the underlying partition when the file system is first formatted or expanded. It will not utilize storage from the free space available on the file system (for example, free space reported by df).

If you receive the following failure message during the dedupe conversion process, this indicates that additional scratch space needs to be setup.

2013-03-11 09:15:49.744-04:00 1 MMB1 fs-convert-to-support-dedupe request for evs12-fs-d01-tgt: Checking if sufficient space is free on target file system... 2013-03-11 09:15:49.744-04:00 1 MMB1 fs-convert-to-support-dedupe request for evs12-fs-d01-tgt: Scratch space requires 4.21 GB. 2.31 GB is available. 2013-03-11 09:15:49.744-04:00 1 MMB1 fs-convert-to-support-dedupe request for evs12-fs-d01-tgt: Expand the file system size before re-submitting the conversion

You can resolve this issue by expanding the file system. Usually one chunk is all that is required. Any storage beyond what is required for the scratch space from the chunk will be made available to the file system. Once this has been done, you can retry the conversion process.
Viewing the deduplication file system page

To view the Deduplication file system page:
Procedure


The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File System Name</td>
<td>Use to search by file system name.</td>
</tr>
<tr>
<td>EVS</td>
<td>Use to search by a particular EVS</td>
</tr>
</tbody>
</table>
| Show               | Use to search by type of file system version:  
  - Dedupe Supported  
  - Dedupe not supported  
  - All file systems  
  
Filter              | Use to initiate your search criteria.                                                                                                                                                                |
| File Systems       | Displays a list of file systems that match the search criteria.                                                                                                                                     |
| Used Capacity      | Displays the total amount of file system space in use, in GB and as a percentage of the total.                                                                                                          |
| Reclaimed Capacity | Displays the space savings based on deduplication, presented in bytes and in a percentage. The percentage is the ratio of the Deduped column to the sum of Deduped and Use' columns. Note that the dedupe process begins by taking a temporary snapshot of the file system and then dedupes it. |
| Status             | Displays the status:                                                                                                                                                                                |
Enabling dedupe for a file system

To enable dedupe for a file system:

Procedure

2. Enter the search criteria in the Filter section of the page and then click Filter.
3. Under the File System label, fill the check box next to the file system to be enabled. You can enable one or more file systems at a time.
4. Click enable.
   The system immediately starts the dedupe-enable process. The Status column displays Enabled to reflect this action.

Converting a file system to enable dedupe

You can convert an existing WFS-2 file system to support and enable dedupe. After the conversion process takes place, the file system is dedupe-enabled. Converting a file system can take some time and it is recommended that you plan accordingly for the conversion time. It is recommended that you convert one file system at a time. See the fs-convert-to-support-dedupe man
page for important information and considerations before starting the conversion process. For example:

- The file system should be in an unmounted state.
- The file system must have sufficient space.
- The file system should not have any object-based snapshots.

**Procedure**

2. Select **Dedupe not supported** from the **Show** list to display file systems do not have dedupe support enabled.
3. Click **Filter**.
4. The system displays the file systems that need conversion in order to be dedupe-enabled.
5. Fill in the check box next to the file system to convert. It is recommended that you one file system at a time.
6. Click **Convert** and read the messages in the dialog that appears.
7. After you have read the message and ensure that you want to proceed with conversion, click **OK**.
8. Click **Active Tasks** to view the current conversion status. After the conversion is done, the file system is dedupe capable and the file system is now queued for a full dedupe run. The dedupe process will start when the file system is queued for dedupe. The Status column displays Enabled.

If the status remains in the Needs Conversion status, check the Events page. Navigate to **Home > Status & Monitoring > Event Log**. This log reports any conversion errors. For example, an error may occur if there is not sufficient space for the file system to be converted, if there are existing object-based snapshots, or if the user-data-write-policy of the file system is set to anything other than never-overwrite. See the following CLI man page for more information:

**wfs-user-data-write-policy**

---

**Using WORM file systems**

A file system is designated as WORM at the time of creation. When creating a WORM file system, start with a non-strict WORM file system to test your retention policy; then, when you are ready to deploy a compliance solution, create a strict WORM file system.

**Note:** Any existing non-WORM file system can be reformatted as a WORM file system. Reformatting a file system to use a different file system type must be done at the CLI. For detailed information on this process, run **man format**.
**Designating retention date**

Before you mark a file as WORM, designate its retention date. To configure the retention date, set the file's last access time to a specific time in the future. The last access time can be set using the UNIX `touch` command; for example:

```
touch -a MMDDhhmm[YY] ./filename
```

Should the retention date be less than or equal to the current time, it will never expire.

Once a file has been marked as WORM, that file’s permissions cannot be altered until the file reaches its retention date. Once a WORM file reaches its retention date, you can read the contents of the file, or delete the entire file, but its permissions cannot be changed to allow read-write access. When write access is granted, the file can be deleted; however, the contents of the file will still remain unavailable for modification.

**Marking a file as WORM**

Once the retention date has been set, a file can be marked as WORM. To mark a file as WORM, set the permissions of the file to read-only:

- From a UNIX client, remove the write attribute permissions.
- From a Windows client, mark the file as read-only through the file’s properties.

**Managing virtual volumes**

A file system can be divided into discrete areas of storage called virtual volumes. From a client’s perspective, a virtual volume appears to be a normal file system. Virtual volumes provide a simple method for allocating and controlling directories for projects, users, or groups. Capacity and number of files within the virtual volume can be controlled using quotas.

**Viewing virtual volumes**

Lists all the current virtual volumes for the EVS and file system named and allows the virtual volume’s details to be viewed.
Procedure

1. Navigate to the **Home > Storage Management > Virtual Volumes & Quotas** to display the **Virtual Volumes & Quotas** page.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS/File System</td>
<td>The name of the selected EVS and file system.</td>
</tr>
<tr>
<td>Filter</td>
<td>Filters can be defined to reduce the number of virtual volumes displayed on the page and can be configured based on the name or the path.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the virtual volume.</td>
</tr>
<tr>
<td>File System</td>
<td>Name of the file system.</td>
</tr>
<tr>
<td>Contact</td>
<td>Contact email address for information and alerts about virtual volume activity.</td>
</tr>
<tr>
<td>Path</td>
<td>Directory on which the virtual volume has been created.</td>
</tr>
<tr>
<td>Usage</td>
<td>Amount of data in the virtual volume.</td>
</tr>
<tr>
<td>details</td>
<td>Displays the <strong>Virtual Volumes</strong> page for the selected virtual volume.</td>
</tr>
<tr>
<td>add</td>
<td>Displays the <strong>Add Virtual Volume</strong> page.</td>
</tr>
<tr>
<td>delete</td>
<td>Displays the <strong>Delete Virtual Volume</strong> page.</td>
</tr>
<tr>
<td>View Quotas</td>
<td>Deletes one or more virtual volumes.</td>
</tr>
</tbody>
</table>

**Note:** Only the first contact email address is shown; to view the full set of contacts or to modify the virtual volume, click **details**.
Adding a virtual volume

**Procedure**

1. Navigate to **Home > Storage Management > Virtual Volumes & Quotas**
2. Click **add** to display the **Add Virtual Volume** page.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS/File System</td>
<td>The EVS and the file system to which to add this virtual volume. If the volume will be added to a different EVS/file system, click change and select an EVS/file system.</td>
</tr>
<tr>
<td>Virtual Volume Name</td>
<td>The name of the virtual volume.</td>
</tr>
<tr>
<td>Create a CIFS Share or NFS Export with the same name as the virtual volume</td>
<td>If a share or export with the same name as the virtual volume does not exist, selecting this check box ensures its creation. This is only intended for convenience in accessing the virtual volume through CIFS or NFS.</td>
</tr>
<tr>
<td>Allow exports to overlap</td>
<td>As overlapping exports can potentially expose security loopholes, the condition can be tested for and, if found, the export creation can be denied.</td>
</tr>
<tr>
<td>Path</td>
<td>Directory in the file system that will be the root of the virtual volume; for example, /company/sales. All subdirectories of this path will be a part of this volume.</td>
</tr>
<tr>
<td></td>
<td>The path to the directory at the root of the virtual volume must be specified, or selected by browsing the file system. If the directory does not yet exist, then leaving the box checked will ensure it is created. It should be noted that if the system is left to create the directory in this way, the owner will be designated 'root', and the default quotas for this virtual volume will be named anonymously.</td>
</tr>
<tr>
<td>Email Contacts</td>
<td>Email contacts to receive information about virtual volume usage.</td>
</tr>
<tr>
<td><strong>OK</strong></td>
<td>Saves configuration changes, and closes the page.</td>
</tr>
</tbody>
</table>
### Field/Item Description

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cancel</td>
<td>Closes the page without saving configuration changes.</td>
</tr>
</tbody>
</table>

3. In the **Virtual Volume Name** field, enter the name. Note the following:
   - The name can be up to 128 characters.
   - Do not use the characters `?*=+[];:/,<>\` in the name.
   - The name A$ is reserved for the Windows Event Viewer, and cannot be used.

4. If a CIFS share of the same name as this virtual volume is required, fill the **Create a CIFS Share with the same name as the Virtual Volume** check box. Selecting this check box ensures its creation.

5. If an NFS export with the same name as the virtual volume is required, fill in the **Create a NFS Export with the same name as the Virtual Volume** check box.

6. If there is a possibility that this new NFS export will overlap an existing export, fill in the **Allow exports to overlap** check box.

7. Enter the path to the directory at the root of the virtual volume or click **Browse** and navigate to the file system path.

8. If the directory does not yet exist, fill in the **Create path if it does not exist** check box to ensure that it is created.

9. Enter each email address in the **Email Contacts** box, and click **add** to append it to the list. Email lists are limited to a maximum of 512 characters.

   - **To configure email notification of threshold alerts**, designate explicit email recipients (for example, admin@company.com) to receive email notification any time a defined threshold has been reached.
   - **To send email to all affected user accounts when their user quota has been reached**, add an email address beginning with * to the Email Contacts list (for example, *@company.com).

Note: If no email contacts are specified for the virtual volume, the server generates events for quota warnings. To generate events in addition to email alerts, go to the server’s command line interface and issue the command `quota-event--on`.

10. **Click OK.**

### Modifying a virtual volume

Describes how to modify the name and email address of an existing virtual volume.
Procedure

1. Navigate to **Home > Storage Management > Virtual Volumes & Quotas** to display the **Virtual Volumes & Quotas** page.
2. Click **details** to display the **Virtual Volume** page.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS/File System</td>
<td>The EVS and the file system to which to add this virtual volume. If the virtual volume will be added to a different EVS/file system, click change and select an EVS/file system.</td>
</tr>
<tr>
<td>Virtual Volume Name</td>
<td>The name of the virtual volume.</td>
</tr>
<tr>
<td>Path</td>
<td>Directory in the file system that is the root of the virtual volume; for example, /company/sales. All subdirectories of this path will be a part of this volume.</td>
</tr>
<tr>
<td>Security Mode</td>
<td>Displays the <strong>File System Security</strong> page.</td>
</tr>
<tr>
<td>Total Quota Limits Allocated</td>
<td>Displays the total quota limits allocated.</td>
</tr>
<tr>
<td>Total Usage</td>
<td>Displays the total usage.</td>
</tr>
<tr>
<td>File Count</td>
<td>Displays the file count.</td>
</tr>
<tr>
<td>Email Contacts</td>
<td>Displays existing email contacts.</td>
</tr>
<tr>
<td><strong>OK</strong></td>
<td>Saves configuration changes, and closes the page.</td>
</tr>
<tr>
<td><strong>cancel</strong></td>
<td>Closes the page without saving configuration changes.</td>
</tr>
<tr>
<td>View Corresponding Share</td>
<td>Displays the corresponding shares.</td>
</tr>
<tr>
<td>View Corresponding Export</td>
<td>Displays the corresponding exports.</td>
</tr>
<tr>
<td>Data Migration Paths</td>
<td>Displays the <strong>Data Migration Paths</strong> page.</td>
</tr>
</tbody>
</table>

3. To modify the virtual volume name, enter the new name.
4. To add new email contacts, enter the email address and click **add**. To delete an existing email address, select the address from the list and click **x**.

5. Click **OK**.

**Deleting a virtual volume**

A virtual volume can only be removed from a directory when the directory is empty. To delete a virtual volume that is assigned to a directory that contains data, first remove the data, then delete the volume.

**Procedure**

1. Navigate to **Home > Storage Management > Virtual Volumes & Quotas**.
2. Select one or more virtual volumes.
3. Click **delete**.
   
   A warning message displays asking for confirmation that this action is definitely required.
4. Click **OK**.

**Managing quotas on virtual volumes**

Three types of quotas are maintained for each virtual volume:

- **Explicit User/Group Quotas**. A quota explicitly created to impose restrictions on an individual user or group, defining a unique set of thresholds.

- **Default User/Group Quotas**. A quota set automatically for all users and groups that do not have explicit quotas, set by defining a set of Quota Defaults (thresholds) for creating a quota automatically when a file is created or modified in the virtual volume.

  Default quotas for virtual volumes operate in the same way as those defined for file systems. User (Group) quota defaults define a set of thresholds for creating a quota for a user (or group) the first time that user (or group) saves a file in the virtual volume.

  Initially, quota defaults are not set. When activity occurs in the virtual volume, it is tracked, but quotas are not automatically created. When at least one threshold is set to a non-zero value, a User or Group quota (as appropriate) will be created for the owner of the directory at the root of the virtual volume.

- **Virtual Volumes & Quotas**. A virtual volume quota tracks the space used within a specific directory on the virtual volume. A quota can be explicitly created to define a set of thresholds restricting all operations in the virtual volume, unrelated to which user or group initiated them.

---

**Note:** Quotas track the number and total size of all files. At specified thresholds, emails alert the list of contacts associated with the virtual volume.
and, optionally, *Quota Threshold Exceeded* events are logged. Operations that would take the user or group beyond the configured limit can be disallowed by setting hard limits.

When *Usage* and *File Count* limits are combined, the server will enforce the first quota to be reached.

**Viewing and modifying virtual volume quotas**
This page lists all the current quotas for the specified virtual volume or the specified file systems, and allows a quota's details to be viewed.

**Procedure**

1. Navigate to **Home > Storage Management > Virtual Volumes & Quotas**.
2. Fill in the check box next to the virtual volume to view or modify and then click **View Quotas** to display the **Quotas** page.

![Quotas page](image)

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| Virtual Volume                | Identifies the virtual volume to which these quotas apply:  
  - **EVS/File System**: EVS and file system on which the virtual volume resides.  
  - **Virtual Volume Name**: Name of the virtual volume.  
  - **Path**: Directory on which the virtual volume has been created. |
| Filter                        | Because many user/group quotas can exist on a virtual volume, the server provides a way to filter the list.  
  - Filter Types: You can select from All Types (default), Users or Groups.  
  - in which User/Group Account matches: In this field, enter a name to be matched. The wildcard character * may be used. |
| User/Group Account (also known as the target) | A quota name can consist of:  
  - A CIFS domain and user or group name, such as bb\Smith or bb \my_group (where bb is a domain, Smith is a user and my_group is a group).  
  - An NFS user or group such as richardb or finance (in which richardb is an NFS user and finance is an NFS group).  
  - A name can be empty (if the quota is a virtual volume quota) or 0 (if the quota was created for the owner of the directory at the root of the virtual volume). |
<p>| Quota Type                    | Type of source of virtual volume activity. Possible values are User, Group, or Virtual Volume . The type applies to anyone initiating activity in the entire virtual volume, and only one quota with this target type may exist on each virtual volume. |
| Created By                    | Method of quota creation. Possible values are <strong>Automatically Created</strong> (created using a quota default) or <strong>User Defined</strong> (where the quota was set uniquely for one particular quota). |
| Usage Limit                   | Overall limit set for the total size of all files in the virtual volume owned by the target of the quota. |</p>
<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Count Limit</td>
<td>Overall limit set for the total number of files in the virtual volume owned by the target of the quota.</td>
</tr>
<tr>
<td>add</td>
<td>Displays the Add Quota page.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes a selected quota.</td>
</tr>
<tr>
<td>refresh cache</td>
<td>Clears the SMU’s cache and repopulates the cache with the relevant objects. (This is different than clicking the browser refresh button, which picks up any recent updates without clearing the cache.)</td>
</tr>
<tr>
<td>User Defaults</td>
<td>Advances to the User Quota Defaults page, in which you can set or change the defaults for users.</td>
</tr>
<tr>
<td>Group Defaults</td>
<td>Advances to the User Quota Defaults page, in which you can set or change the defaults for groups.</td>
</tr>
<tr>
<td>Download Quotas for this Virtual Volume</td>
<td>Downloads a comma-separated value (CSV) file containing all available quota information for the virtual volume.</td>
</tr>
</tbody>
</table>

**Setting user/group defaults**

This procedure illustrates the User Default page. The Group Default page is identical, except for the Automatically create quotas for Domain Users check box. This option allows default quotas for the group Domain Users to be created. By default, every NT user belongs to the group Domain Users, which includes every NT user in the quota unless each user’s primary group has been explicitly set.

**Procedure**

1. Navigate to Home > Storage Management> Virtual Volumes & Quotas to display the Quotas page.
2. Click **User Defaults** to display the **User Quota Defaults** page.

![User Quota Defaults Page](image)

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS/File System</td>
<td>The EVS and file system on which the user quota applies.</td>
</tr>
<tr>
<td>Virtual Volumes</td>
<td>Name of the virtual volume to which a user quota created using these defaults is assigned.</td>
</tr>
<tr>
<td><strong>Usage</strong></td>
<td></td>
</tr>
<tr>
<td>Limit</td>
<td>Amount of space to enable in Bytes: KB, MB, GB or TB.</td>
</tr>
<tr>
<td>Hard Limit</td>
<td>When enabled, the amount of space specified in the Limit field cannot be exceeded.</td>
</tr>
<tr>
<td>Warning</td>
<td>Percentage of the amount of space specified in the Limit field at which a Warning alert will be sent.</td>
</tr>
<tr>
<td>Severe</td>
<td>Percentage of the amount of space specified in the Limit field at which a Severe alert will be sent.</td>
</tr>
<tr>
<td><strong>File Count</strong></td>
<td></td>
</tr>
<tr>
<td>Limit</td>
<td>Maximum number of files to allow in this virtual volume.</td>
</tr>
<tr>
<td>Hard Limit</td>
<td>When enabled, the number of files specified in the Limit field cannot be exceeded.</td>
</tr>
<tr>
<td>Warning</td>
<td>Percentage of the number of files specified in the Limit field at which a Warning alert will be sent.</td>
</tr>
<tr>
<td>Severe</td>
<td>Percentage of the number of files specified in the Limit field at which a Severe alert will be sent.</td>
</tr>
<tr>
<td>Log Quota Events in the managed server's Event log</td>
<td>Filling this check box sets the default for all users or groups to have quota events logged in the server’s event log.</td>
</tr>
</tbody>
</table>
### Deleting a virtual volume

A virtual volume can only be removed from a directory when the directory is empty. To delete a virtual volume that is assigned to a directory that contains data, first remove the data, then delete the volume.

**Procedure**

1. Navigate to **Home > Storage Management > Virtual Volumes & Quotas**.
2. Select one or more virtual volumes.
3. Click **delete**.

   A warning message displays asking for confirmation that this action is definitely required.

4. Click **OK**.

### Exporting quotas for a specific virtual volume

**Procedure**

1. Navigate to **Home > Storage Management > Virtual Volumes & Quotas** to display the **Virtual Volumes & Quotas** page.
2. Select a virtual volume and click **View Quotas** to display the **Quotas** page.
3. Click **Download Quotas for this Virtual Volume**.
4. Save the quota information to as a comma-separated value (CSV) file. You also can choose to display the quota information in an application.
Managing file system security

Security modes can be configured per-cluster/server, per-file system, or per-virtual volume. Selecting security modes on a tiered basis, rather than system-wide, enhances the granularity and convenience of managing system security.

- Viewing security considerations
**Viewing security considerations**

This page displays all EVSs and the configured security mode. Security modes can be configured per-EVS, per-file system, or per-Virtual Volume. This page can list all the EVSs or a particular EVS, and show the file systems based on the selections made on the page, and the filter is defined.
**Procedure**

1. Navigate to **Home > File Services > File System Security** to display the **File System Security** page.

![File System Security Page](image)

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS Security Context</td>
<td>Displays the currently selected EVS security context.</td>
</tr>
<tr>
<td><strong>change</strong></td>
<td>Selects a different EVS security context. You can select either Global Configuration which applies to all EVSs, or select a specific EVS.</td>
</tr>
<tr>
<td>EVS Security Mode</td>
<td>Displays current EVS security mode settings, and allows you to change those settings.</td>
</tr>
<tr>
<td>Default File System Security Mode</td>
<td>Indicates the default security mode that is in effect for the entire EVS. Click the <strong>Switch Mode</strong> link to switch the security mode for the entire EVS. You can switch between <em>Mixed mode</em> and <em>UNIX mode</em>.</td>
</tr>
<tr>
<td><strong>Filter</strong></td>
<td>Control the information displayed in this page. In the <strong>File Systems</strong> field, select whether to show file systems. In the <strong>Virtual Volumes</strong> field, select whether to show virtual volumes. Click <strong>filter</strong> to refresh the page based on the criteria selected in these two fields.</td>
</tr>
<tr>
<td>EVS</td>
<td>List of all virtual servers (EVSs) defined by the filter.</td>
</tr>
<tr>
<td>File System</td>
<td><em>If this column is blank</em>, the displayed security mode is associated with the EVS.</td>
</tr>
<tr>
<td></td>
<td><em>If this column displays a file system label</em>, the displayed security mode is associated with this specific file system.</td>
</tr>
<tr>
<td>Virtual Volume</td>
<td>Lists the virtual volumes found on the file systems defined by the filter.</td>
</tr>
<tr>
<td>Field/Item</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Mode</td>
<td>Security mode defined on the EVS or file system. File systems without an explicit security mode configuration inherit security mode from the EVS.</td>
</tr>
<tr>
<td>details</td>
<td>Advances to the Security Configuration page in which the security mode for the selected EVS can be modified.</td>
</tr>
<tr>
<td>CIFS Setup</td>
<td>Advances to a page in which CIFS setup can be performed.</td>
</tr>
</tbody>
</table>

**NFS security and Kerberos**

The NAS server supports Kerberos to provide authentication, integrity, and privacy when using NFS v2, v3, and v4. Kerberos provides a mechanism for entities (principals) to authenticate to each other and securely exchange session keys. The NAS server supports RPCSEC_GSS using Kerberos v5.

The HNAS Kerberos implementation has been updated with the Advanced Encryption Standard (AES). The Data Encryption Standard (DES) has been deprecated and is not secure.

Secure NFS requires configuration of the NFS server’s Kerberos principal name, and secret keys. Kerberos related configuration settings are setup both globally and on a per-EVS basis. The NFS host name is configured on a per-EVS basis.

**Setting secure NFS**

NFS supports three secure options:
- krb5: provides authentication only
- krb5i: provides authentication and integrity
- krb5p: provides authentication, integrity, and privacy (encryption of data)

NFS exports can be set to accept only secure connections. This is done by specifying the appropriate security options in the Access Configuration field of the Add Export page or the NFS Export Details page.

Setting the type of secure connections can be done using the CLI command `nfs-export` with the `mod -c` option. See the Command Line Reference for more information.

**Mixed security mode**

The server’s mixed security mode supports both Windows and UNIX security definitions. Security is set up uniquely on each file (or directory), based on which user created, or last took ownership of, the file (or directory). If a Windows user, the security definition will be native CIFS and subject to
Windows security rules; likewise, if a UNIX user, the security definition will be native NFS and subject to UNIX security rules.

**CIFS access to native CIFS files**

When a CIFS client tries to access a native CIFS file (that is, with Windows security information), the server checks the user information against the file’s security information to determine whether an operation is permissible:

- **User Security.** This information is contained in an access token, which is made up of the user security identifier (SID), primary group SID, and other SIDs. The server receives the token from the domain controller and caches it for use throughout the user’s session.

- **File Security.** This information is contained in a file’s security descriptor, which is made up of the owner SID, group SID, and access control list (ACL). The ACL can contain several access control entries (ACEs), which specify the conditions for access.

ACE entries can be modified or deleted using a set of CLI commands called the `cacls` commands. This set of commands includes `cacls-add`, `cacls-del`, `cacls-fields`, `cacls-mask-in`, `cacls-mask-out`, and `cacls-set`. For more information on these commands, refer to the *Command Line Reference*.

**NFS access to native NFS files**

When an NFS client tries to access a native NFS file (with UNIX security information), the server checks the user’s UNIX credentials against the file’s security information to determine whether or not an operation is permissible. The file security information is made up of a user ID, group ID, and read, write, and execute permissions.

**Client access to non-native files**

CIFS users may access files which have UNIX security information, and NFS users may access files which have Windows security information. The server supports this functionality with mapping tables, set up in the Web Manager, that associate the names of NFS users and groups with their Windows equivalents. For example, when a CIFS user tries to access a file that has UNIX-only security information, the server automatically maps the user name to the corresponding NFS name in the mapping table.

- The server automatically translates user security information from UNIX to Windows format, or vice-versa, and caches it for the duration of the session:

<table>
<thead>
<tr>
<th>UNIX credential</th>
<th>NT access token</th>
</tr>
</thead>
<tbody>
<tr>
<td>UID</td>
<td>User mapping table</td>
</tr>
<tr>
<td></td>
<td>User SID</td>
</tr>
<tr>
<td>UNIX credential</td>
<td>NT access token</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>GID</td>
<td>Group mapping table</td>
</tr>
<tr>
<td>Other groups</td>
<td>Group mapping table</td>
</tr>
<tr>
<td></td>
<td>Other groups</td>
</tr>
</tbody>
</table>

- The system automatically converts file security attributes from Windows to UNIX format and stores the result in file metadata, making the files native to both CIFS and NFS clients. Although UNIX files are also converted to Windows format, the results are not stored in file metadata:

- Any changes that a user makes to a file’s security attributes are applied equally to Windows and UNIX. When a CIFS user tries to access a file that has UNIX-only security information, the server maps the user to an NFS name and converts the user’s access token to UNIX credentials. It then checks these credentials against the file’s security attributes to determine whether or not the operation is permissible. Similarly, when an NFS user tries to access a file that has Windows-only security information, the server maps the user to a Windows name and converts the user’s UNIX credentials to a Windows access token. It then checks the token against the file’s security attributes.

**UNIX security mode**

When the server is configured in UNIX security mode, it supports UNIX security for CIFS and NFS clients. However, all security settings are saved with UNIX file attributes. As a result, NFS clients are always accessing files in native mode, while CIFS clients are always accessing file non-native mode.
Note: With UNIX security mode, NFS users do not need to rely on the presence of a Windows domain controller (DC) in order to access files. As a result, they are fully isolated from potential DC failures.

Changing security modes

By default, the virtual volume or file system inherits the parent file system's security mode. In other words, when the parent file system has a UNIX security mode, the virtual volume associated with the file system will inherit the UNIX security mode. This page can be used to modify the inherited security mode for the selected virtual volume.

Procedure

2. Click details to display the Security Configuration page.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS</td>
<td>Displays the selected virtual volume's parent EVS.</td>
</tr>
<tr>
<td>File System</td>
<td>Displays the selected virtual volume's parent file system (when selected from the File System Security page filter options).</td>
</tr>
<tr>
<td>Virtual Volume</td>
<td>Displays the selected virtual volume whose security mode can be changed (when selected from the File System Security page filter options).</td>
</tr>
<tr>
<td>Mode</td>
<td>The security mode defined on the virtual volume or file system, depending on the selection from the File System Security page filter options).</td>
</tr>
<tr>
<td>OK</td>
<td>Saves configuration changes, and closes the page.</td>
</tr>
<tr>
<td>cancel</td>
<td>Closes the page without saving configuration changes.</td>
</tr>
</tbody>
</table>

3. Select a security mode from the Mode list.
4. Click OK.

Mixed mode operation

The storage server allows network clients to share a common pool of storage on both Windows and UNIX clients. This is called mixed mode operation. Although the server does this as seamlessly as possible, the two protocols are considerably different, so mixed mode operation presents some challenges, discussed in the File Name Representation and Symbolic Links sections.
File name representation

The maximum length of a file name is 255 characters, and file names may contain any Unicode character. Case-sensitivity in file names is significant to NFS and FTP clients, but not SMB clients.

Modern Windows clients (NT and newer) can make full use of UCS-2 (a two byte Unicode encoding). When communicating with Windows 9x, the server uses the Latin-1 version of extended ASCII.

When communicating with NFS clients, the server supports Latin-1 and UTF-8. The Latin-1 character set is the default for NFS clients. If you plan to have file names that include non-ASCII characters, you should change the default encoding used by the server using the protocol-character-set command.

Symbolic links

Symbolic links (symlinks) are commonly used:

- To aggregate disparate parts of the file system.
- As a convenience, similar to a shortcut in the Windows environment.
- To access data outside of a cluster. For example, a symlink can point to data in another server in a server farm or a non-Hitachi Data Systems server.

There are two types of symlinks:

- **Relative symlinks** contain a path relative to the symlink itself. For example, .. ./dst is a relative symlink.
- **Absolute symlinks** contain a path relative to the root of the file system on the NFS client that created the symlink (not relative to the root of the server's file system). For example, /mnt/datadir/dst is an absolute symlink.

When accessing the file system through NFS, the server fully supports symlinks. NFS/UNIX clients assume that files marked as symbolic links contain a text pathname that the client can read and interpret as an indirect reference to another file or directory. Any client can follow a symlink, but accessing the target file (or directory) still requires permission.

As of CIFS clients, however, are not able to follow files marked as symlinks, so the server provides a server-side symlink following capability. When a CIFS or FTP client accesses a server-side symlink, the server reads the path from the link and attempts to follow it automatically:

- **For relative symlinks**, the link can be followed, because the server can follow the path from the link itself.
- **For absolute symlinks**, however, the server does not have access to the root of the file system on the NFS client that created the link, and is therefore not able to follow the link automatically.
To allow SMB2 clients to access shares, the server provides global symlinks, which allow CIFS clients to follow absolute symlinks:
- If an absolute symlink refers to a file or directory in the same CIFS share as the symlink, the server follows the symlink (on behalf of the CIFS client) internally.
- If an absolute symlink refers to an object in a different CIFS share to the symlink, the CIFS client is redirected to the link’s destination via the Microsoft’s DFS mechanism.

**Note:** Microsoft’s DFS mechanism only supports redirection to a directory (not a file), therefore, absolute symlinks that refer to a file (in a different CIFS share) will not be handled properly by a CIFS client.

The link’s destination may be on the same file system as the link, on a different file system within a server farm, or on a remote CIFS server. To associate a global symlink with an absolute symlink, the server maintains a translation table between absolute symlink paths and global symlink paths.

**Note:** As of release 12.2 of the Hitachi NAS Platform, CIFS2 clients using SMB2 or higher are able to follow relative symlinks to files on storage without the use of global symlinks.

When accessing server-side symlinks, CIFS clients cannot follow some symlinks which are perfectly valid for NFS, because the storage system follows the symlink on the CIFS client’s behalf and presents the linked-to file instead of the symlink. In this case, in line with the behavior of Samba, the server hides the existence of the symlink entirely from the CIFS/FTP client. By default, a symlink that points outside of the scope of its own share (for example, to a different file system) are not followed.

Global symlinks (also called absolute symlinks) start with a slash character (/), and they allow you to set up links to data outside a cluster. NFS clients follow the global symlink directly and, for CIFS clients, the server maintains a server-side translation table, that allows those clients to access the symlink destination. Both NFS and CIFS clients can follow the same global symlink to the destination directory, when the global symlink, the exports, shares, and mount points are set up correctly. When a client encounters a global symlink:
- **For NFS clients**, the server returns the content of the global symlink, allowing the client to follow the link to the destination. This means that the NFS client’s mount points and the NFS exports must be set up correctly.
- **For CIFS clients**, the server causes the client to request a symlink lookup from the local EVS translation table. Once the client requests the lookup, the server returns the destination server name, share name, and path to the CIFS client, allowing it to access the destination.
Using global symlinks with CIFS has a performance penalty. Therefore, global symlinks are disabled by default, but can be enabled by filling the Follow Global Symbolic Links check box on the Add Share page (when creating the share) or CIFS Share Details page (after the share has been created).

Symlink translation tables are maintained on a per-EVS basis, meaning that:

- **Table entries do migrate with the EVS.** If an EVS is migrated, all of its table entries migrate along with the EVS.
- **Table entries do not replicate from the EVS.** When replicating data from one EVS to another, the mapping information for global symlinks is not automatically relocated, and it must be recreated in the translation table of the EVS into which the data was copied.
- **Table entries do not move with a file system.** If a file system is moved from one EVS to another, the mapping information for global symlinks is not automatically relocated and must be manually adjusted, except for those symlinks that are relative to a CNS tree (those symlinks do not require adjustment).
- **Table entries irrelevant for symlinks that are relative to a CNS.** When an EVS is migrated, no adjustment is necessary for symlinks that are relative to a CNS because, when the client follows the symbolic link, it is first referred to the CNS tree, then from the CNS tree to a real file system when the path crosses a CNS link.

The symlink translation table is managed via the following CLI commands:

- `global-symlink-add`
- `global-symlink-del`
- `global-symlink-delall`
- `global-symlink-list`

Refer to the *Command Line Reference* for information about the CLI commands used to manage global symlinks.

### Mixed mode operation and LDAP servers

The storage server supports mixed mode access for file systems, meaning that a mapping is required between the file system permissions and owns in order to ensure consistent security and access. NIS/LDAP services allow the server to locate and map users and permissions based on an existing NIS/LDAP service on the network, instead of creating a local account on the storage server.
On an existing LDAP service, one of the following methods will typically be used for allowing the server to locate and map users and permissions:

- **RFC 2307 Schema**
  
  RFC 2307 defines a standard convention for the storage and retrieval of user and group mapping information from an LDAP server. If your site uses RFC 2307 schema, and you configure your storage server/cluster to support both mixed mode operations and LDAP services, it is assumed that you have already loaded the RFC 2307 schema into your directory, and that you have already provisioned the user objects appropriately.

- **Services for UNIX (SFU) schema**
  
  If you have configured SFU (Services for UNIX), you must explicitly enable NIS participation for each account in the active directory (AD) domain. You can enable NIS participation for an individual account on the UNIX Attributes tab of the user account properties in the Active Directory Users and Computers utility.

To ensure optimum performance when your server/cluster is configured to support both mixed mode operations and LDAP services, the most optimized configuration includes the creation of indexes in the LDAP service for attributes queried by the storage server. To ensure fastest responses to queries, exact-match indexes should be configured on the LDAP server for the attributes to be searched. The LDAP server on your network should index at least the following attributes:

<table>
<thead>
<tr>
<th>Objects that:</th>
<th>RFC 2307 Class</th>
<th>Services for UNIX Class</th>
<th>Map to NIS Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Describe user accounts</td>
<td>posixAccount</td>
<td>user</td>
<td>posixAccount</td>
</tr>
<tr>
<td>Describe the group identifier</td>
<td>posixGroup</td>
<td>group</td>
<td>posixGroup</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attributes for:</th>
<th>RFC 2307 Attribute</th>
<th>Services for UNIX Attribute</th>
<th>Map to NIS Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID/login name</td>
<td>uid</td>
<td>sAMAccountName</td>
<td>memberUid</td>
</tr>
<tr>
<td>User ID number</td>
<td>uidNumber</td>
<td>msSFU30UidNumber</td>
<td>uidNumber</td>
</tr>
<tr>
<td>Group name</td>
<td>cn</td>
<td>cn</td>
<td>memberNisNetgroup</td>
</tr>
<tr>
<td>Group ID number</td>
<td>gidNumber</td>
<td>msSFU30GidNumber</td>
<td>gidNumber</td>
</tr>
</tbody>
</table>

The RFC 2307 or Services for UNIX attributes may or may not be previously indexed on the LDAP server, depending on the distributor of the director services.

To track indexing performance, you can use the `ldap-stats` command, which permits you to monitor response times for LDAP queries. It is necessary to first let the storage server complete some successful user lookups so that
some statistical data can be gathered. In a short period of time, however, you should be able to determine whether any of the attributes are not indexed.

**Mandatory and advisory byte-range file locks in mixed mode**

The HNAS server supports both SMB and NFS locks. The HNAS server supports only one type of byte range locking for SMB clients. For NFS clients, however, additional byte range lock types are supported. When created by NFSv2 and NFSv3 clients, the HNAS server supports both monitored (NLM/NSM) and non-monitored advisory byte-range locks. When created by NFSv4 clients, the HNAS server supports both mandatory and advisory byte range locks.

The following tables describe the HNAS server behavior when a client locks a file using a byte range lock:

- **Server default configuration (the HNAS server treats byte range locks by NFSv4 clients as mandatory):**

<table>
<thead>
<tr>
<th>Locked by client of type</th>
<th>Lock type when the client accessing the locked file is:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>NFSv2 or NFSv3</td>
</tr>
<tr>
<td>NFSv2 or NFSv3</td>
<td>Advisory</td>
</tr>
<tr>
<td>NFSv4</td>
<td>Mandatory</td>
</tr>
<tr>
<td>SMB</td>
<td>Mandatory</td>
</tr>
</tbody>
</table>

- **When the HNAS server is configured to treat byte range locks from NFSv4 clients as advisory:**

<table>
<thead>
<tr>
<th>Locked by client of type</th>
<th>Lock type when the client accessing the locked file is:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>NFSv2 or NFSv3</td>
</tr>
<tr>
<td>NFSv2 or NFSv3</td>
<td>Advisory</td>
</tr>
<tr>
<td>NFSv4</td>
<td>Advisory</td>
</tr>
<tr>
<td>SMB</td>
<td>Mandatory</td>
</tr>
</tbody>
</table>

To change the HNAS server configuration so that it treats NFSv4 byte-range locks as advisory, use the command `set nfsv4-locking-is-advisory-only 1`.

To change the HNAS server configuration so that it treats NFSv4 byte-range locks as mandatory, use the command `set nfsv4-locking-is-advisory-only 0`.

**Opportunistic locks (oplocks)**

An oplock is a performance-enhancing technique used in Microsoft networking (CIFS) environments. It enables applications to speed up file
access and minimize network traffic by caching all or part of a file locally. As
the data is kept on the client, read and write operations can be performed
locally, without involving the server.

The server supports three categories of oplocks:

- **Exclusive.** An Exclusive oplock enables a single client to cache a file for
  both *reading and writing*. As the client that owns the oplock is the only
  client accessing the file, it can read and modify all or part of the file locally.
  The client does not need to post any changes to the server until it closes
  the file and releases the oplock.

- **Batch.** A Batch oplock enables a single client to cache a file for both
  *reading and writing*, as in the case of an exclusive oplock. In addition, the
  client can preserve the cached information even after closing the file; file
  open and close operations are also performed locally. The client does not
  need to post any changes back to the server until it releases the oplock.

- **Level II.** A Level II oplock enables multiple clients to cache a file for
  *reading only*. The clients owning the oplock can read file data and
  attributes from local information, cached or read-ahead. If one client
  makes any changes to the file, all the oplocks are broken.

When dealing with oplocks, the server acts in accordance with the CIFS
specification. Whether operating in a pure Windows environment or with a
mix of CIFS and NFS clients, the server allows applications to take advantage
of local caches while preserving data integrity.

**Exclusive and batch oplocks**

An Exclusive or Batch oplock is an exclusive (read-write/deny-all) file lock
that a CIFS client may obtain at the time it opens a file. The server grants
the oplock only if no other application is currently accessing the file.

When a client owns an Exclusive or Batch oplock on a file, it can cache part
or all of the file locally. Any changes that the client makes to the file are also
cached locally. Changes do not need to be written to the server until the
client releases the oplock. In the case of an Exclusive oplock, the client
releases the oplock when the server requests that it does so, or when it
closes the file. In the case of a Batch oplock, the client may keep information
(including changes) locally even after closing the file. While the client has an
Exclusive or Batch oplock on a file, the server guarantees that no other client
may access the file.

If a client requests access to a file that has an Exclusive or Batch oplock, the
server asks the client with the oplock to release it. The client then writes the
changes to the server and releases the oplock. Once this operation has
finished, the server allows the second client to access the file. This happens
regardless of the second client’s network protocol.
In cases where a CIFS client requests an oplock on a file that has an Exclusive or Batch oplock, the server breaks the existing oplock and grants both clients Level II oplocks instead.

**Level II oplocks**

A Level II oplock is a non-exclusive (read-only/deny-write) file lock that a CIFS client may obtain at the time it opens a file. The server grants the oplock only if all other applications currently accessing the file also possess Level II oplocks:

- *If another client owns an Exclusive or Batch oplock*, the server breaks it and converts it to a Level II oplock before the new client is granted the oplock.
- *If a client owns a Level II oplock on a file*, it can cache part or all of the file locally. The clients owning the oplock can read file data and attributes from local information without involving the server, which guarantees that no other client may write to the file.
- *If a client wants to write to a file that has a Level II oplock*, the server asks the client that has the oplock to release it, then allows the second client to perform the write. This happens regardless of the network protocol that the second client uses.

**User and group names in NFSv4**

In NFSv4 users and groups are identified by UTF-8 strings of the form: `user@dns_domain` and `group@dns_domain`. The NAS Platform supports the following universal user/group identifiers:

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OWNER@</td>
<td>The owner of a file.</td>
</tr>
<tr>
<td>GROUP@</td>
<td>A file’s group.</td>
</tr>
<tr>
<td>EVERYONE@</td>
<td>The world.</td>
</tr>
<tr>
<td>NETWORK@</td>
<td>Accessed via the network.</td>
</tr>
<tr>
<td>ANONYMOUS@</td>
<td>Accessed without any authentication.</td>
</tr>
<tr>
<td>AUTHENTICATED@</td>
<td>Any authenticated user.</td>
</tr>
</tbody>
</table>

**Configuring user and group mappings**

When the server is operating in either mixed or UNIX security mode, it creates mappings between UNIX and Windows users and groups. For example, user John Doe could have a UNIX user account named `jdoe` and a Windows user account named `johnd`. These two user accounts are made equivalent by setting up a user mapping. Furthermore, the server assumes that equivalent user and group names are the same for both environments. For example, if no explicit mapping is found for user `janed`, the server assumes that the UNIX user account named `janed` is the same as the Windows user account with the same name.
There are two steps to follow when setting up user and group mappings on the server:

- Specify each NFS user and group’s name and ID. Note that this step is not required for Windows users or groups, as the server obtains all of the information it needs from the domain controller (DC).
- Map the NFS user (group) names to Windows NT user (group) names.

**Managing NFS user and group mapping**

Windows access to a file created by a UNIX user (or vice-versa) is permitted when the UNIX name and Windows name are recognized as being the same user. However, NFS clients present an NFS operation to an NFS server with numerical UNIX User ID (UID) and UNIX Group ID (GID) as credentials. The server must map the UID and GID to a UNIX user or group name prior to verifying the UNIX to Windows name mapping.

The server uses the following methods to map from a numerical UNIX UID or GID to a UNIX user name or group name:

- If the server is configured to use the Network Information Service (NIS) no special configuration steps are needed; the server automatically retrieves the user (group) names and IDs from the NIS server.
- NFS user and group names can be added manually.
- NFS user and group names can be added by importing files. For example, the UNIX /etc/passwd file can be imported, providing the server with a mapping of user name to UID. The /etc/groups file should also be imported to provide the server with a mapping of Group name to GID.
- You can import the numerical ID to Name mappings directly from a NIS server or an LDAP server if one has been configured. Every time a UID is presented to the server, it will issue an NIS request to an NIS server to verify the mapping. This mapping can remain cached in the server for a configurable time. A cached ID to name binding for a User or Group will appear as Transient in the NFS Users or Groups list.

---

**Note:** When a Windows user creates a file and the UNIX user or group mapping fails, the server sets the UID or the GID to 0 (root). In previous releases, the server sets the UID or GID to 0 (root) or to 65534 (nobody).

**Viewing NFS user mappings**

Each UNIX user name and numerical UID can be manually entered, along with its corresponding Windows user and domain name. Users configured manually will appear as permanent in the NFS users list.
Procedure

1. Navigate to **Home > File Services > User Mapping** to display the **User Mapping** page.

The fields and items on this page are described in the table below:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS Security Context</td>
<td>Displays the currently selected EVS security context. Click <strong>change</strong> to select a different EVS security context or to select the global configuration. Selecting a different EVS security context changes the EVS to which the mapping applies.</td>
</tr>
</tbody>
</table>
| Filter                | Filter the list of user mappings using any of the following criteria:  
  - **Name**, which applies to the NFSv2/v3, NFSv4 user names or the Windows user name.  
  - **UID**, which can be used to specify a range of UID values to display, or a minimum/maximum UID value to display.  
  - Fill the **Show Discovered Information** check box to display only information that has been discovered from NIS servers, LDAP servers, or domain controllers. |
| NFSv2/3 Name          | User name configured in the UNIX environment.                                                                                                                                                  |
| UID                   | User ID configured in the UNIX environment.                                                                                                                                                     |
| Windows Name          | User name configured in the Windows environment.                                                                                                                                               |
| NFSv4 Name            | Displays the NFSv4 user name.                                                                                                                                                                  |
| Kerberos Name         | Displays the Kerberos principal (of the form user@realm) for the user.                                                                                                                         |
### Field/Item

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>details</td>
<td>Changes the properties of a mapping, or to display more detailed information about a mapping.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes the selected mapping.</td>
</tr>
<tr>
<td>refresh cache</td>
<td>Clears the SMU’s cache, and then repopulates the cache with the relevant objects.</td>
</tr>
</tbody>
</table>

**Note:** This is different than clicking the browser refresh button, which picks up any recent updates without clearing the cache.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh Mappings</td>
<td>Refreshes the mappings without clearing the cache.</td>
</tr>
<tr>
<td>Import Users</td>
<td>Opens the <a href="#">Import User Mappings</a> page.</td>
</tr>
<tr>
<td>View Domain Mapping</td>
<td>Opens the <a href="#">Domain Mappings</a> page.</td>
</tr>
<tr>
<td>Group Mappings</td>
<td>Opens the <a href="#">Group Mappings</a> page.</td>
</tr>
</tbody>
</table>

2. **If necessary, click change to select a different EVS security context or to select the global configuration.**

   The EVS Security Context displays the currently selected EVS security context. Changes made to mappings using this page apply only to the currently selected EVS security context.

   - If an EVS uses the Global configuration, any changes made to the global configuration settings will affect the EVS.
   - If an EVS uses an Individual security context, changes made to the global configuration settings will not affect the EVS. To change the mappings of an EVS using an individual security context, you must select the EVS' individual security context to make changes, even if those settings are the same as the settings used by the global security context.

### Creating an NFS user mapping

Each UNIX user name and numerical UID can be manually entered, along with its corresponding Windows user and domain name. Users configured manually will appear as permanent in the NFS users list.

**Procedure**

1. Navigate to **Home > File Services > User Mapping** to display the [User Mapping](#) page.
2. Click **add** to display the **Add User Mapping** page.

The following table describes the fields and items on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFS v2/3</td>
<td>The NFS user account name.</td>
</tr>
<tr>
<td>UID</td>
<td>The Unix user identifier.</td>
</tr>
<tr>
<td>Windows Name</td>
<td>The Windows user account name.</td>
</tr>
<tr>
<td>Windows ID</td>
<td>The Windows group identifier.</td>
</tr>
<tr>
<td>NFSv4 Name</td>
<td>The NFSv4 user name.</td>
</tr>
<tr>
<td>Kerberos Name</td>
<td>The Kerberos principal (of the form user@realm) for the user.</td>
</tr>
<tr>
<td>OK</td>
<td>Saves configuration changes, and closes the page.</td>
</tr>
<tr>
<td>cancel</td>
<td>Closes the page without saving configuration changes.</td>
</tr>
</tbody>
</table>

3. Fill the check box under each selection as appropriate:
   - **Save to NAS server** - The server relies on information you provide.
   - **Discover** - The server relies on information discovered from NIS servers, LDAP servers, or domain controllers for this mapping.
   - **Ignore** - The server will not try to retrieve that information from NIS servers, LDAP servers, or domain controllers

**Modifying user mappings**

**Procedure**

1. Navigate to **Home > File Services > User Mapping**.
2. Fill the check box on the user mapping to modify and then click **details** to display the **User Mapping Details** page.
<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFS v2/3 Name</td>
<td>Displays the NFSv2/3 user account name.</td>
</tr>
<tr>
<td>Unix ID</td>
<td>Displays the UNIX user identifier.</td>
</tr>
<tr>
<td>Windows Name</td>
<td>Displays the Windows user account name.</td>
</tr>
<tr>
<td>Windows ID</td>
<td>Displays the Windows identifier.</td>
</tr>
<tr>
<td>NFSv4 Name</td>
<td>Displays the NFSv4 user name.</td>
</tr>
<tr>
<td>Kerberos Name</td>
<td>Displays the Kerberos principal (of the form user@realm) for the user.</td>
</tr>
<tr>
<td>OK</td>
<td>Saves configuration changes, and closes the page.</td>
</tr>
<tr>
<td>cancel</td>
<td>Closes the page without saving configuration changes.</td>
</tr>
</tbody>
</table>

3. Make any changes as necessary to the fields described in the table.
   - **Save to NAS server** - The server relies on information you provide.
   - **Discover** - The server relies on information discovered from NIS servers, LDAP servers, or domain controllers for this mapping.
   - **Ignore** - The server will not try to retrieve that information from NIS servers, LDAP servers, or domain controllers

**Deleting a user mapping**

**Procedure**

1. Navigate to Home > File Services > User Mapping to display the User Mapping page.
2. Fill the check box next to the NFSv2/3 name of the user mapping to delete, and click delete.
3. Click OK to confirm the deletion.

**Adding group mappings manually**

This page allows you to create a group mapping by entering account information in the given fields.

**Procedure**

1. Navigate to Home > File Services > Group Mappings to display the Group Mappings page.
2. Click **add** to display the **Add Group Mapping** page.

![Add Group Mapping](image)

The following table describes the items and fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFSv2/3 Name</td>
<td>Enter the NFS group account name.</td>
</tr>
<tr>
<td>Group ID</td>
<td>Enter the UNIX group identifier.</td>
</tr>
<tr>
<td>Windows Name</td>
<td>Enter the Windows group account name.</td>
</tr>
<tr>
<td>Windows ID</td>
<td>Enter the Windows group identifier.</td>
</tr>
<tr>
<td>NFSv4 Name</td>
<td>Enter the NFSv4 group account name.</td>
</tr>
<tr>
<td><strong>OK</strong></td>
<td>Saves configuration changes, and closes the page.</td>
</tr>
<tr>
<td><strong>cancel</strong></td>
<td>Closes the page without saving configuration changes.</td>
</tr>
</tbody>
</table>

3. Fill the check box under each selection as appropriate:

- **Save to NAS server** - The server relies on information you provide.
- **Discover** - The server relies on information discovered from NIS servers, LDAP servers, or domain controllers for this mapping.
- **Ignore** - The server will not try to retrieve that information from NIS servers, LDAP servers, or domain controllers

**Modifying group mappings**

This page allows you to make changes to the group mapping.

**Procedure**

1. Navigate to **Home > File Services > Group Mappings**.
2. Fill the check box next to the group mapping to modify, and click **details** to display the **Group Mapping Details** page.
The following table describes the items and fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFSv2/3 Name</td>
<td>NFS group account name.</td>
</tr>
<tr>
<td>Group ID</td>
<td>UNIX group identifier.</td>
</tr>
<tr>
<td>Windows Name</td>
<td>Windows group account name.</td>
</tr>
<tr>
<td>Windows ID</td>
<td>Windows group identifier.</td>
</tr>
<tr>
<td>NFSv4 Name</td>
<td>NFSv4 group account name.</td>
</tr>
<tr>
<td>OK</td>
<td>Saves configuration changes, and closes the page.</td>
</tr>
<tr>
<td>cancel</td>
<td>Closes the page without saving configuration changes.</td>
</tr>
</tbody>
</table>

3. Make changes as necessary and click **OK**.

**Deleting a group mapping**

To delete a group mapping:

**Procedure**

1. Navigate to **Home > File Services > Group Mappings**.
2. Fill the check box next the group mapping to delete, and click **delete**.
3. To confirm the deletion, click **OK**.

**About importing user or group mappings from a file or an NIS LDAP server**

You can specify user or group details by importing them from a file.

NFSv4 user and group names are distinct from the UNIX name associated with UNIX UIDs and GIDs. However, in many environments a user/group’s NFSv4 name can be derived from their UNIX name by appending the NFSv4 domain. The storage server can perform this conversion automatically, based on the settings specified on the Domain Mappings page of Web Manager or through the CLI command domain-mappings-add.

To display the Domain Mappings page, navigate to Home > File Services, select User Mapping or Group Mapping, and select the View Domain Mapping link. For more information on the `domain-mappings-add` command, refer to the **Command Line Reference**.

A UNIX `/etc/passwd` file can be imported, providing the server with a mapping of user name to UID. The `/etc/groups` file should also be imported to provide the server with a mapping of Group name to GID.

The server will ignore other fields from the `passwd` file, such as the encrypted password and the user’s home directory. Users or Groups configured by importing from the `/etc/passwd` file will then appear in the appropriate list on the User Mappings page or the Group Mappings page.
Choose one of the three following formats and use it consistently throughout the file:

- **NFSv2/3 user/group data only.** The source of the user data can be a UNIX password file, such as `/etc/passwd`.
  When using Network Information Service (NIS), use the following command to create the file:
  
  ```bash
  ypcat passwd > /tmp/x.pwd
  ```
  The resulting file has the following format:
  
  ```text
  john:x:544:511:John Brown:/home/john:/bin/bash
  keith:x:545:517:Keith Black:/home/keith:/bin/bash
  miles:x:546:504:Miles Pink:/home/miles:/bin/bash
  carla:x:548:504:Carla Blue:/home/carla:/bin/bash
  ```

- **NFSv2/3-to-Windows user/group mappings only.** Create a file with entries in the following format:
  
  ```text
  UNIXuser="NT User", "NT Domain"
  ```
  with the following syntax rules:
  
  - NT domain is optional.
  - NFS user names cannot contain spaces.
  - NT names must be enclosed in quotation marks.
  - If the domain name is omitted, the server domain is assumed. If the empty domain name is required, it must be specified like this:
    ```text
    users=“Everyone”, “”
    ```
    where the Everyone user is the only common account with an empty domain name.

- **Both NFSv2/3 user/group data and NFSv2/3-to-Windows user mappings.** Create a file with entries in the following format:
  
  ```text
  UNIXUser:UNIXid="NT User", "NT Domain"
  ```
  with the same rules for NFS and NT names as for the NFSv2/3-to-Windows user mapping.
  The resulting file has entries in the following format:
  
  ```text
  john:544="john", “Domain1”
  keith:545="keith", “Domain1”
  miles:546="miles", “Domain1”
  carla:548="carla", “Domain1”
  ```

### Importing a user mapping from a file or an NIS or LDSP server

You can import a mapping from a file stored on your machine or on a network drive.

**Procedure**

1. Navigate to **Home > File Services > User Mapping**.
2. Click **Import Users** to display the **Import User Mapping** page.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import From File</td>
<td>Import a mapping from a file stored on your machine or on a network drive. Search for the file by clicking <strong>Browse</strong>, and then click <strong>Import</strong>.</td>
</tr>
<tr>
<td>Import From NIS/LDAP</td>
<td>Import a mapping from the currently used NIS/LDAP server by clicking <strong>Import</strong>.</td>
</tr>
</tbody>
</table>

3. Complete the import process by choosing one of the following:

- To import from a file, enter the file name in the **Filename** field or click **Browse** to locate the file, and then click **Import**.
- To import from NIS/LDAP, click **Import**. The NIS or LDAP server displayed in the Current Domain will be contacted, and the mappings will be imported.

**Importing a group mapping from a file or an NIS LDAP server**

This topic describes how to import group mappings from a file stored on your machine or on a network drive, and to import group mappings from an NIS/LDAP server.

**Procedure**

1. Navigate to **Home > File Services > Group Mappings**.
2. Click **Import Groups** to display the **Import Group Mappings** page.

The following table describes how the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import From File</td>
<td>Import a mapping from a file stored on your machine or on a network drive. Search for the file by clicking <strong>Browse</strong>, and then click <strong>Import</strong>.</td>
</tr>
<tr>
<td>Import From NIS/ LDAP</td>
<td>Import a mapping from the currently used NIS/LDAP server by clicking <strong>Import</strong>.</td>
</tr>
</tbody>
</table>

3. Complete the import process by choosing one of the following:

- To import from a file, enter the file name in the **Filename** field or click **Browse** to locate the file, and then click **Import**.
- To import from NIS/LDAP, click **Import**. The NIS or LDAP server displayed in the Current Domain will be contacted, and the mappings will be imported.
Sharing resources with NFS clients

A fundamental component of most UNIX networks, the Network File System (NFS) protocol provides PC and UNIX workstations with transparent access to one another’s files. This section describes how to set up NFS exports, and explains about NFS statistics, supported clients, and prerequisites.

The server implements the file-serving functions of an NFS server, providing normal file-serving functions, such as:

- Export manipulation
- File manipulation (read, write, link, create, and so forth)
- Directory manipulation (mkdir, readdir, lookup, and so forth)
- Byte-range file locking
- File access control (permissions)
- File and directory attributes (sizes, access times, and so forth)
- Hard links and symbolic (soft) links

- [Enabling NFS Protocol Support](#)
- [Supported NFS versions](#)
- [Configuring NFS exports](#)
- [About the rquotad service](#)
Enabling NFS Protocol Support

To enable NFS access to the system:
- Enter an NFS license key.
- Enable the NFS service.

Supported clients and protocols

The NAS server/cluster supports all clients compliant with NFS version 2, version 3, or version 4 standards. NFS version 2 and version 3 support includes both TCP and UDP, but NFS version 4 support includes TCP only. The server/cluster also supports the following UNIX protocols:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Supported versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFS</td>
<td>2, 3, and 4</td>
</tr>
<tr>
<td>Port Mapper</td>
<td>2</td>
</tr>
<tr>
<td>Mount</td>
<td>1 and 3</td>
</tr>
<tr>
<td>Network Lock Manager (NLM)</td>
<td>1, 3, and 4</td>
</tr>
<tr>
<td>Network Status Monitor (NSM)</td>
<td>1</td>
</tr>
</tbody>
</table>

NFS statistics

NFS statistics for the HNAS server (in 10-second time slices) are available for activity since the previous reboot, or since the point when statistics were last reset.

Supported NFS versions

The storage server supports NFS versions 2, 3, and 4. Both TCP and UDP are supported in versions 2 and 3, but version 4 support is for TCP only. By default, the maximum version supported is version 3, meaning that the server supports versions 2 and 3 by default. To change the maximum supported version to NFSv4, use the CLI command `nfs-max-supported-version`. By setting the maximum supported version to 4, you allow the storage server to support NFS versions 2, 3, and 4.

Statistics for NFS client connections are kept, and can be viewed on the NFS Statistics page (refer to the Server and Cluster Administration Guide for more information).
**NFS V2/V3 and NIS unicode support**

When using NFSv2/3 to communicate with clients/devices and/or NIS servers, the default character set is ISO 8859-1 (Latin-1). This character set may not be sufficient to communicate with both NFS clients and NIS servers (for example, when characters outside the Latin-1 range are required, such as Chinese, Japanese or Korean), so an administrator can specify the character set(s) to be used when communicating with NFS clients and/or NIS servers using the `protocol-character-set` command. The `protocol-character-set` command specifies which character set is used when sending/receiving:

- File and directory names to/from NFS clients.
- User and group names to/from NIS servers.

Communication with all NFS clients and/or all NIS servers uses the same character set; you cannot specify that the storage server/cluster communicates with some NFS clients or some NIS servers using one character set, and other NFS clients or NIS servers using a different character set.

**Changing the character set**

By default, the storage server/cluster uses the ISO 8859-1 (Latin-1) character set when communicating with NFS clients and/or NIS servers. When NIS servers and NFS clients use different character sets, the administrator must specify which character set the NFS clients are using, and which character set the NIS servers are using.

The `protocol-character-set` command allows an administrator to specify the character set to be used when communicating with NFS clients and/or NIS servers. Refer to the *Command Line Reference* for more information on the `protocol-character-set` command.

---

**Note:** After the `protocol-character-set` command is issued, the specified character set is put into use immediately, without the need to restart the server/cluster.

**Unicode support**

The storage server (or cluster) stores metadata about the files, directories, migration paths, CIFS shares, NFS exports, user names, group names, log entries, mount points and so on for the virtual servers, file systems, and name spaces served by the server/cluster.

When interacting with another network device, the metadata transmitted to or received by the storage server/cluster must be encoded in a character set supported by the other network device. Typically, clients/devices using the
CIFS (Windows) protocol encode data in the UCS-2 character set, and clients/devices that use the NFS protocol encode data in the UTF-8 character set.

**Note:** The data on storage subsystems attached to a storage server/cluster is not affected in any way by the character sets currently used by the server/cluster.

When using the FTP protocol to communicate with clients/devices, the storage server/cluster supports the UTF-8 character encoding for user names, passwords, and file/directory names.

### Enabling and disabling file services

Describes how to enable and disable the desired file services for the system.

**Procedure**

1. Navigate to **Home > File Services > Enable File Services** to display the **Enable File Services** page.

2. Select or deselect one or more services.

3. Click **apply**.

<table>
<thead>
<tr>
<th>Fields/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• CIFS/Windows</td>
<td>Fill the check box for each service you want to enable.</td>
</tr>
<tr>
<td>• NFS/UNIX</td>
<td></td>
</tr>
<tr>
<td>• FTP</td>
<td></td>
</tr>
<tr>
<td>• iSCSI</td>
<td></td>
</tr>
<tr>
<td>• CNS</td>
<td></td>
</tr>
<tr>
<td>• ReadCache</td>
<td></td>
</tr>
</tbody>
</table>

* A reboot may be required to start/stop this service.

The following table describes the fields on this page:
Notes:

- With the exception of FTP, these services require a valid license to enable the service.
- If ReadCache is selected or deselected, a reboot may be required. If so, then follow the on-screen instructions to restart the server.

Configuring NFS exports

NFS exports are configured on mounted file systems. NFS exports can be configured manually or export details can be imported from a file. NFS exports can be configured manually or by importing the details from a file.

The NFSv4 pseudo file system

NFSv4 introduces the concept of the pseudo file system, where exports appear as directories. NFSv4 clients do not connect directly to NFS exports as in NFSv2/3. Instead all clients connect to the root of the pseudo file system, which is a virtual directory. The pseudo file system is generated automatically from the NFS exports, and is maintained automatically as exports are modified and removed. You can choose to present all the file systems in a single pseudo file system.

The HNAS server allows you to create views of many file systems from one point of contact, name spaces. These views are available on a per EVS basis or for the entire cluster.

This is an example of a pseudo file system:

A server named **numbers** has two exports: `/one` and `/two`. If a client wishes to get access to export `/one`, there are two ways to mount exports:

```
mount -t nfs4 numbers:/ /mnt
```

which mounts the pseudo file system at `/mnt`

```
mount -t nfs4 numbers:/one /mnt
```

which mounts the export `/one` at `/mnt`

The first method is only supported in NFSv4. The second method is supported in versions 2, 3, and 4. In the first method, the client can export `/one` with the command `cd /mnt/one`, and to export `/two` with `cd /mnt/two`. 

## Kerberos configuration

### Prerequisites

**Note:** The HNAS Kerberos implementation has been updated with the Advanced Encryption Standard (AES). The Data Encryption Standard (DES) has been deprecated and is not secure. AES pre-requisites are:

- Windows Server 2008 or higher is required to deploy a Microsoft Windows KDC.
- Configuration may be required on the clients. The configuration of the KDC and clients may vary depending on their operating systems.
- The Kerberos Principle accounts on the KDC may need to be configured to support AES.
- Supported AES encryption types are
  - AES256: HMAC-SHA1-96
  - AES128: HMAC-SHA1-96

Configuring the HNAS server requires the following steps:

### Procedure

1. Create the principal and key of the service (the EVS) on the KDC (Key Distribution Center).

   The keytab file must contain the service principal for the NFS service for the EVS. Once the NFS service principal for the EVS has been added, you can then create a keytab file specifically for the EVS. The type of key is critical.

   - **AES:** To use AES, the HNAS keytab must contain an AES key to enable AES by default. If an AES only keytab is imported, DES is disabled. If an AES only keytab is imported, all clients must be configured to support AES and have an AES key in their keytabs.
   - **DES:**
     - To use DES, the client must perform the Kerberos authentication with any of the supported encryption types except AES.
     - The HNAS must have a key that corresponds to whatever encryption type the client used.
   - **AES** and **DES:** The keytab must contain
     - An AES key and
     - Any old supported encryption type key (it does not have to be DES), provided that it is supported by the client as well.

For example, with an EVS named “man” in the Kerberos realm **AESIR.EXAMPLE.COM**, the keytab file for the NFS service on “man” should contain a principal **nfs/man.aesir.example.com@AESIR.EXAMPLE.COM**.
The format of the principal starts with the service (nfs), followed by a slash, then the fully-qualified-domain name of the EVS, then the symbol @, and finally the Kerberos realm. (Note that case is significant. Kerberos realms are always in uppercase. Also, there must be no trailing period after the Kerberos realm.)

2. Export a keytab file from the KDC.
   Typically you will use the kadmin utility run from the master KDC to export a keytab file. For details on creating an appropriate keytab file, refer to the documentation for the tools supplied with your version of Kerberos.

3. Import the keytab file into the HNAS server.
   Transfer the keytab file to the flash of the HNAS server.
   For example: securely move the keytab file to the SMU and transfer it to the NAS server. Log on with ssc, and do the following:

   SERVER:$ ssput man.nfs.keytab man.nfs.keytab

   The first name is the local file name on the SMU, the second name is the name to use on the server. Once the file has been placed on the server, import the keytab in the context of the EVS with:

   SERVER:$ krb5-keytab import man.nfs.keytab

   After the keytab has been imported, the uploaded keytab file can be safely removed with:

   SERVER:$ ssrm man.nfs.keytab

4. Set the Kerberos realm for the HNAS server.
   Set the realm by using the command krb5-realm. For example:

   SERVER:$ krb5-realm AESIR.EXAMPLE.COM

   After performing these steps, the NAS server is able to complete the configuration. However, you may choose to create mappings between the Kerberos users/groups and the Active Directory users/groups.

Viewing NFS exports

This page provides details of existing NFS exports and allows you to add, modify and delete them. This page can be configured to display all the exports associated with:
- The global cluster name space (CNS)
- An individual name space for an EVS
- A specific file system
Procedure

1. Navigate to **Home > File Services > NFS Exports** to display the **NFS Exports** page.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS/File System</td>
<td>The name of the EVS and the file system to which the NFS export is assigned. To display the NFS exports of a different EVS or file system, click <strong>change</strong>.</td>
</tr>
<tr>
<td>Filter</td>
<td>Allows the table to be filtered by name and path. Click <strong>filter</strong> to display the NFS export table.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the NFS export.</td>
</tr>
<tr>
<td>File System</td>
<td>The name of the file system (or CNS link to a file system) to which the NFS exports is assigned.</td>
</tr>
<tr>
<td>Path</td>
<td>The path and directory to which the NFS export is directed.</td>
</tr>
<tr>
<td>details</td>
<td>Opens the <strong>NFS Export Details</strong> page in which you can display detailed information about the NFS export.</td>
</tr>
<tr>
<td>add</td>
<td>Advances to the <strong>Add Export</strong> page.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes the selected NFS export.</td>
</tr>
<tr>
<td>refresh cache</td>
<td>Clears the SMU's cache, and then repopulates it with the relevant objects. Note that this is different than clicking the browser refresh button, which picks up any recent updates without clearing the cache.</td>
</tr>
</tbody>
</table>
| Download Exports | Downloads a CSV file containing a list of all configured NFS exports on the selected EVS and file system. Note that the downloaded file cannot be used to restore NFS exports (you must restore NFS sharing resources with NFS clients

Hitachi NAS Platform File Services Administration Guide

121
<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>exports from an NFS exports backup file). To download a list of exports from another file system, click <strong>change</strong>.</td>
</tr>
<tr>
<td><strong>Backup &amp; Restore</strong></td>
<td>Displays the <strong>NFS Export Backup &amp; Restore</strong> page.</td>
</tr>
<tr>
<td><strong>Read Cache Options</strong></td>
<td>Advances to the <strong>Read Cache Options</strong> page.</td>
</tr>
<tr>
<td><strong>Read Cache Statistics</strong></td>
<td>Advances to the <strong>Read Cache Statistics</strong> page.</td>
</tr>
</tbody>
</table>

### Adding an NFS export

**Procedure**

1. Navigate to **Home > File Services > NFS Exports** to display the **NFS Exports** page.
2. Click **add** to display the **Add Export** page.

The following table describes the fields on page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS/File System</td>
<td>Currently selected EVS and file system, to which the NFS Export will link.</td>
</tr>
<tr>
<td>Export Name</td>
<td>Name of the export.</td>
</tr>
<tr>
<td>Path</td>
<td>Path to the source directory for the export.</td>
</tr>
<tr>
<td>Path Options</td>
<td>Determines the path options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Create path if it does not exist</strong> to create the path entered in the Path field.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Allow this export to overlap other exports</strong> if nested NFS exports are allowed.</td>
</tr>
<tr>
<td>Show snapshots</td>
<td>Determines how to show snapshots:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Show and Allow Access</strong>, to display and allow access to snapshots.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hide and Allow Access</strong>, to hide snapshots, but still allow access to the hidden snapshots.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hide and Disable Access</strong>, to hide and disallow access to snapshots.</td>
</tr>
<tr>
<td>Local Read Cache</td>
<td>Allows caching of files or cross file system links from the file system to which this export points:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Cache all files</strong>, Allows caching of files and cross file system links in the file system of the export. Cross file system links are local links that point</td>
</tr>
</tbody>
</table>
### Field/Item Description

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>to a data file in a remote file system. The remote file system may be on a remote server or storage device.</td>
<td>- Cache cross-file system links. Allows only cross file system links to be cached  &lt;br&gt; - Do not cache files. Do not allow read caching of files and cross file system links.  &lt;br&gt; Local read caching is not supported for NFSv4 clients.</td>
</tr>
<tr>
<td>Transfer to Object Replication Target</td>
<td>When a file system is recovered from a snapshot, one of the final steps is to import the NFS exports found in the snapshot representing the selected version of the file system. Only those NFS exports marked as transferable will be imported.  &lt;br&gt; - Enable: NFS exports will be transferred to recovered file systems.  &lt;br&gt; - Disable: NFS exports will not be transferred to recovered file systems.  &lt;br&gt; - Use FS default: When the target file system is brought online, NFS exports will be transferred if Transfer Access Points During Object Replication option is enabled for the file system.</td>
</tr>
<tr>
<td>Access Configuration</td>
<td>IP addresses, host names, or the NIS netgroups of the clients who are allowed to access the NFS export (up to 5957 characters). If the system has been set up to work with a name server, you can enter the NIS netgroup to which the clients belong, or the client’s computer name rather than its IP address (not case sensitive). You can also specify the flavor of NFS security using the option ( \text{sec}=&lt;\text{mode}&gt; ).</td>
</tr>
</tbody>
</table>

**OK** Saves configuration changes, and closes the page.  <br>**cancel** Closes the page without saving configuration changes.

3. To add an export to a new EVS or file system, click change next to that line and make a selection from the Select a File System page.

4. Enter the Export Name through which clients will access the export.

5. Type the path to the directory being exported or click browse... to locate an existing directory.

6. Set Path Options as follows:
   - To create the path automatically when it does not already exist, fill the Create path if it does not exist check box.

   **Note:** Automatically created directories will be owned by the root user and group (UID:0 / GID:0) and will be accessible to all users (that is, the permissions are set to rwxrwxrwx). It is recommended that such directories be created via CIFS or NFS, or that such directories are given the desired permissions explicitly after being created by this option.

   - To allow this export path to overlap other exports, fill the Allow this export path to overlap other exports check box.

   This option is useful if you expect to set up future, nested exports. For example, suppose you export the root directory of a volume and make

---

Sharing resources with NFS clients  <br>Hitachi NAS Platform File Services Administration Guide
it available to managerial staff only. By selecting this option, you can later export subdirectories of the root directory and make each of them available to different groups of users.

7. If snapshots are present, make them visible to clients by selecting from the list:

- **Show and Allow Access**, to display and allow access to snapshots.
- **Hide and Allow Access**, to hide snapshots, but still allow access to the hidden snapshots.
- **Hide and Disable Access**, to hide and disallow access to snapshots.

In order for this change to become effective on NFS clients, all NFS clients should unmount and then remount the export, or the administrator must run `touch .` from within the root directory of the export.

8. Select the Local Read Cache setting. To allow caching of files or cross file system links from the file system to which this export points, select one of the following:

- **Cache all files**. Allows caching of files and cross file system links in the file system of the export. Cross file system links are local links that point to a data file in a remote file system. The remote file system may be on a remote server or storage device.
- **Cache cross-file system links**. Allows only cross file system links to be cached.

Local read caching is not supported for NFSv4 clients.

9. Choose the **Transfer to Object Replication Target** option.

When a file system is recovered from a snapshot, one of the final steps is to import the NFS exports found in the snapshot representing the selected version of the file system. Only those NFS exports marked as transferable will be imported.

Use the list to specify one of the following:

- **Enable**: NFS exports will be transferred to recovered file systems.
- **Disable**: NFS exports will not be transferred to recovered file systems.
- **Use FS default**: When the target file system is brought online, NFS exports will be transferred if Transfer Access Points During Object Replication option is enabled for the file system.

10. In the Access Configuration field, type the IP addresses, host names, or the NIS netgroups of the clients who are allowed to access the NFS export (up to 5,957 characters). If the system has been set up to work with a name server, you can enter the NIS netgroup to which the clients belong, or the client’s computer name rather than its IP address (not case sensitive). You can also specify the flavor of NFS security using the option `(sec=<mode>)`. The table outlines what to type in this field.
### IP address export qualifiers

The following table describes qualifiers that can be appended to IP addresses when specifying client access to an NFS export:

<table>
<thead>
<tr>
<th>Qualifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>read_write, readwrite, rw</td>
<td>Grants read/write access. This is the default setting.</td>
</tr>
<tr>
<td>read_only, readonly, ro</td>
<td>Grants read-only access.</td>
</tr>
<tr>
<td>root_squash, rootsquash</td>
<td>Maps user and group IDs of 0 (zero) to the anonymous user or group. This is the default setting.</td>
</tr>
<tr>
<td>no_root_squash, norootsquash</td>
<td>Turns off root squashing.</td>
</tr>
<tr>
<td>all_squash, allsquash</td>
<td>Maps all user IDs and group IDs to the anonymous user or group.</td>
</tr>
<tr>
<td>no_all_squash, noallsquash</td>
<td>Turns off all squashing. This is the default setting.</td>
</tr>
<tr>
<td>secure</td>
<td>Requires requests to originate from an IP port less than 1024. Access to such ports is normally restricted to administrators of the client machine. To turn it off, use the insecure option.</td>
</tr>
<tr>
<td>insecure</td>
<td>Turns off the secure option. This is the default setting.</td>
</tr>
<tr>
<td>anon_uid, anonuid</td>
<td>Explicitly sets an anonymous user ID.</td>
</tr>
<tr>
<td>anon_gid, anongid</td>
<td>Explicitly sets an anonymous group ID.</td>
</tr>
<tr>
<td>noaccess, no_access</td>
<td>Denies the specified clients access to the export.</td>
</tr>
<tr>
<td>(sec=&lt;mode&gt;)</td>
<td>Allows you to specify the flavor of NFS security, where &lt;mode&gt; is a colon delimited list of allowed security flavors (sys:krb5:krb5i:krb5p).</td>
</tr>
</tbody>
</table>

Here are some examples:
- **10.1.2.38(ro)**
Grants read-only access to the client whose IP address is 10.1.2.38.

- **10.1.2.0/24 (ro)**
  Grants read-only access to all clients whose IP address is within the range 10.1.2.0 to 10.1.2.255.

- **yourcompanydept (ro)**
  Grants read-only access to all members of the NIS group yourcompanydept.

- ***.mycompany.com (ro, anonuid=20)**
  Grants read-only access to all clients whose computer name ends.mycompany.com. All squashed requests are to be treated as if they originated from user ID 20.

- **10.1.*.* (readonly, allsquash, anonuid=10, anongid=10)**
  Grants read-only access to all the matching clients. All requests are squashed to the anonymous user, which is explicitly set as user ID 10 and group ID 10.

- The order in which the entries are specified is important. Take the following two lines:
  
  * *(ro)  
  10.1.2.38 (rw)  

  The first grants read-only access to all clients, whereas the second grants read/write access to the specified client. The second line is redundant, however, as the first line matches all clients. These lines must be transposed to grant write access to 10.1.2.38.

- **10.1.1.*(sec=sys),10.1.2.*(sec=krb5:krb5i:krb5p),*(sec=krb5p)**
  ○ Clients in the 10.1.1.* subnet use sys authentication.
  ○ Clients in the 10.1.2.* subnet to use krb5, krb5i, or krb5p.
  ○ All other clients use krb5p.

---

**Note:** To improve performance, when specifying clients that can access an export, it is recommended that you specify IP addresses or IP address ranges, including those that include wildcards, before specifying host names or NIS netgroups.

---

**Specifying clients by name**

The following list describes how to specify clients by name, and not an IP address.

- **Full Qualified Domain Name Required.**
  Be sure to specify the fully qualified domain name of the client. For example, use aclient.dept.mycompany.com rather than simply aclient.

- **Leading Wildcard Allowed.**
  To specify a partial name, a single wildcard, located at the start of the name, may be used.

- **Export Options Change Requires Remount.**
When the client mounts the NFS export, it determines which export option to apply to a specific client. Subsequent changes to DNS, WINS, or NIS that would resolve the client’s IP address to a different computer name are only applied to mounted exports when the client unmounts the exports and then remounts them.

- **Name Service Order is Significant.**
  Application of export options to a client’s mount request may be affected by the order in which the system applies DNS, WINS, and NIS information to resolve IP addresses. The first service in name order sequence that can resolve the client name supplies the name and searches configuration options for the export.

### Modifying NFS Export Details

This page displays the current export properties of the selected NFS export for either a cluster name space (CNS) or a file system (shown in two different tables). Most of these properties can be changed.

#### Procedure

1. Navigate to **Home > File Services > NFS Exports** to display the **NFS Exports** page.
2. Fill the check box next to the NFS export to display, and click **details** to display the **NFS Export Details** page.

The following table describes the fields and items on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS/File System</td>
<td>Currently selected EVS and file system, to which the NFS Export will link.</td>
</tr>
<tr>
<td>Export Name</td>
<td>Name of the export.</td>
</tr>
<tr>
<td>Path</td>
<td>Path to the source directory for the export.</td>
</tr>
</tbody>
</table>
| Path Options | Determines the path options:  
  - **Create path if it does not exist** to create the path entered in the Path field.  
  - **Allow this export to overlap other exports** if nested NFS exports are allowed. |
| Show snapshots | Determines how to show snapshots:  
  - **Show and Allow Access**, to display and allow access to snapshots.  
  - **Hide and Allow Access**, to hide snapshots, but still allow access to the hidden snapshots.  
  - **Hide and Disable Access**, to hide and disallow access to snapshots. |
| Local Read Cache | Allows caching of files or cross file system links from the file system to which this export points:  
  - **Cache all files**, Allows caching of files and cross file system links in the file system of the export. Cross file system links are local links that point |
Field/Item | Description
--- | ---
 | to a data file in a remote file system. The remote file system may be on a remote server or storage device.
- **Cache cross-file system links.** Allows only cross file system links to be cached
- **Do not cache files.** Do not allow read caching of files and cross file system links.
Local read caching is not supported for NFSv4 clients.

**Transfer to Object Replication Target**

When a file system is recovered from a snapshot, one of the final steps is to import the NFS exports found in the snapshot representing the selected version of the file system. Only those NFS exports marked as transferable will be imported.
- **Enable:** NFS exports will be transferred to recovered file systems.
- **Disable:** NFS exports will not be transferred to recovered file systems.
- **Use FS default:** When the target file system is brought online, NFS exports will be transferred if Transfer Access Points During Object Replication option is enabled for the file system.

**Access Configuration**

IP addresses, host names, or the NIS netgroups of the clients who are allowed to access the NFS export (up to 5957 characters). If the system has been set up to work with a name server, you can enter the NIS netgroup to which the clients belong, or the client’s computer name rather than its IP address (not case sensitive). You can also specify the flavor of NFS security using the option *(sec=<mode>)*. 

**OK**

Saves configuration changes, and closes the page.

**cancel**

Closes the page without saving configuration changes.

3. Make changes as necessary.
4. Click **OK**.

**Deleting an NFS export**

**Caution:** Export Deletion Alert! Before carrying out the instructions that follow for deleting an export, verify that it is not currently being accessed. If an export is deleted while users are accessing it, their NFS sessions will be terminated and any unsaved data may be lost. When replacing a storage enclosure, delete all the exports associated with it. Then, when the replacement enclosure is available, add new exports on the new system drives.

**Procedure**

1. Navigate to **Home > File Services > NFS Exports** to display the **NFS Exports** page.
2. Fill the check box next to the NFS export to delete, and click **delete**.
3. To confirm the deletion, click **OK**.
Backing up or restoring NFS exports

Procedure

1. Navigate to Home > File Services > NFS Exports to display the NFS Exports page.
2. Click Backup & Restore to display the NFS Exports Backup & Restore page.

3. Choose from the following options:
   - To backup, click backup. In the browser, specify the name and location of the backup file, and click OK or Save (the buttons displayed and the method you use to save the backup file depend on the browser you use).
     A backup file name is suggested, but you can customize it. The suggested file name uses the syntax:
     NFS_EXPORTS_date_time.txt, in which date is Month_Day_Year and time is Hour_Minute_Second_[AM or PM]. For example, NFS_EXPORTS_Aug_4_2006_11_09_22_AM.txt.
   - To restore, navigate to the directory in which the backup file is stored, select the file, click Open and then click restore.

About the rquotad service

The rquotad protocol has been implemented as a service on the storage server. It functions as a read-only protocol and is only responsible for reporting information about user and group quotas. Quotas can be created, deleted, or modified through the Storage Management section of the Web Manager.

A UNIX/Linux NFS client can issue the quota command to retrieve information regarding quota usage of a user or group, based on their ID. The retrieved report contains block count, file count, quota limits on both, and
other information (based on options invoked with the command). For accurate syntax, refer to the client’s man pages, as implementation varies between client operating systems.

The server reports only **Hard Limit** quota information through rquotad. Three different quota limitations can be defined:

- User and group quotas to limit **space** and **file quantity** for **individuals** and **groups within a virtual volume**.
- User and group quotas to limit **space** and **file quantity** for **individuals** and **groups within an entire file system**.
- Virtual volume quotas to limit **space** and **file quantity** by a **virtual volume as a whole**.

**Note:** rquotad reports quota usage information on explicitly defined quotas and automatically created (default) quotas. Default quota information will be reported if an explicit quota has not been defined.

The rquotad service can be configured to report quota information using one of two modes:

- **Restrictive mode.** For the user or group specified in the client-side quota command, the rquotad service reports the quota information for the quota with the most constraints.
- **Matching mode.** For the user or group specified in the client-side quota command, the rquotad service reports the quota information for the first quota that meets the parameters defined by the client-side quota command.

**Note:** If the rquotad service is disabled, all requests are rejected with an error code of “EPERM”.

**Restrictive mode operation**

When in Restrictive mode, the rquotad service picks the first applicable quota threshold crossed. It enables the user to determine the amount of data that can be safely recorded against this quota before reaching its Hard Limit. This is the default configuration option for rquotad on the server.

**Note:** The restrictive mode option returns quota information combined from the quota that most restricts usage and the quota that most restricts file count. For example:

If the user quota allowed 10 K of data and 100 files to be added, and the virtual volume quota allowed 100 K of data and 10 files to be added, rquotad would return information stating that 10 K of data and 10 files could be added. Similarly, if the user quota is 10 K of data of which 5 K is used, and the virtual volume quota is 100 K of data of which 99 K is used, rquotad would return information stating that 1 K of data could be added.
The console command `rquotad` is provided to change between the two options, and also to disable access to quota information. For information on how to configure rquotad, refer to the *Command Line Reference*.

### Matching mode operation

When in Matching mode, the rquotad service follows a specific order to find a match for relevant quota information:

- If rquotad returns quota information for a user, it returns the *user’s quota within the virtual volume* if it exists;
- Otherwise, it moves to the *user’s file system quota* if that exists;
- If no file system quota exists for the user, then it will move to the *virtual volume quota*.

In this manner, rquotad keeps checking until a quota is found for the specified user or group. Once the **first** matching quota is found, rquotad stops searching and returns the quota information.

If a user does not have a specifically defined quota in a virtual volume, or in a file system, and the virtual volume quota allows all users 100 K of data and 10 files, rquotad would return information stating that user’s quota is 100 K of data and 10 files. Similarly, if the user has a specified virtual volume quota that is 200 K of data and 20 files, and a file system quota that is 400 K of data and 40 files, rquotad would return information about only the first quota, stating that 200 K of data and 20 files could be added.
Using CIFS for windows access

Windows networks use the Common Internet File System (CIFS) protocol for file sharing between workstations and servers.

- CIFS/SMB protocol support
- Configuring CIFS security
- Assigning CIFS names
- Viewing CIFS Setup
- Joining an Active Directory
- Removing CIFS sever names
- Configuring local groups
- Configuring CIFS shares
- Using Windows server management
- Restoring a previous version of a file
CIFS/SMB protocol support

The server emulates the file-serving functions of Windows NT 4.0, Windows 2000, Windows 2003, and Windows 2008 servers. From the client perspective, the server is indistinguishable from a Windows file server. It provides all of the normal file-serving functions, including:

- Share manipulation (for example: add, list, and delete).
- File manipulation (for example: read, write, create, delete, move, and copy).
- File locking and byte-range locking.
- File access control using standard Windows ACLs.
- File and directory attributes (for example: read-only, and archive).
- Automatic creation of user home directories.

Note: The following CIFS/SMB features are currently unsupported by the HNAS server:

- Windows Extended Attributes (note that this should not be confused with NFS or POSIX xattr)
- BranchCache
- VSS for SMB file shares
- Support for remote management from Server Manager (Windows 2012 and newer)
- SMB2 large read/write MTU (our current implementation is limited to 64KiB)
- SMB3 multi-channel
- SMB3 failover
- SMB3 encryption
- SMB3 directory leasing
- SMB Direct (SMB3 over RDMA)

Prerequisites

To enable CIFS access to the server:
- Enter a CIFS license key.
- Enable the CIFS service.
- Configure the server.

Depending on the security model used on the CIFS network, configure the server using one of the following methods:

<table>
<thead>
<tr>
<th>Security Model</th>
<th>Client Authentication</th>
<th>Configuration Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>NT Domain security</td>
<td>NT 4 only</td>
<td>Add server to NT domain</td>
</tr>
<tr>
<td>Windows 2000, 2003, and 2008 Active Directory</td>
<td>NT 4 only</td>
<td>Add server to NT domain</td>
</tr>
</tbody>
</table>
When configured to join an Active Directory, the server functions the same way as a server added to an NT domain, except that after joining an Active Directory, the server can authenticate clients using the Kerberos protocol as well as NT 4-style authentication. Most modern Windows clients support both authentication methods, though a number of older Windows clients only support NT 4-style authentication.

**Supported clients**

The HNAS server supports platforms and clients that are compliant with CIFS (SMB) versions 1 (the default), 2, 2.1 and 3.

**Domain controller interaction**

The storage server relies on Windows domain controllers to authenticate users and to obtain user information (for example, group membership). The server automatically discovers and connects to the fastest and most reliable domain controllers. Because operating conditions can change over time, the server selects the “best” domain controller every 10 minutes.

By default, when authenticating clients in an Active Directory, the server uses the time maintained by the domain controller, automatically adjusting for any clock inconsistencies.

**Dynamic DNS**

The storage server supports DNS and DDNS. For more information, refer to the *Network Administration Guide*.

**CIFS Statistics**

CIFS statistics for the storage server (in 10-second time slices) are available for activity since the previous reboot or since the point when statistics were last reset.

**Supported CIFS/SMB versions**

The storage server supports CIFS (SMB) versions 1, 2, 2.1 and 3. SMB version 2 and version 3 support is provided to maintain compatibility with computers running the Windows Vista and Windows Server 2008 operating systems. When using the CIFS protocol to communicate with clients/devices, the storage server/cluster supports the UCS-2 character encoding.

The default SMB version is dependent on the HNAS server version:
SMB2 support is limited to the file server portion of the protocol. When acting as a client (for example, when making domain controller and virus scanner connections), the HNAS server uses only the SMB version 1 client implementation. To enable SMB2 support, use the CLI command `cifs-smb2-enable`. After being enabled, the EVS supports CIFS clients connecting through version 1 or version 2 of the protocol. When enabled, SMB2 or SMB3 support is on a per-EVS basis, it is not server or cluster-wide, meaning that SMB2 or SMB3 support must be specifically enabled on each EVS to which clients may need to connect using that version of the SMB (CIFS) protocol.

<table>
<thead>
<tr>
<th>Server version</th>
<th>Default CIFS/SMB version</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.2 and earlier</td>
<td>SMB1</td>
</tr>
<tr>
<td>11.3 and later</td>
<td>SMB2</td>
</tr>
</tbody>
</table>

**Notes:**

- A valid CIFS license is required in order to enable SMB2 support. For more information about license keys, refer to the *Server and Cluster Administration Guide*.
- When SMB2 support is enabled, the type of CIFS connection established is determined based on the connection type that the client advertises it supports. Only clients advertising support for CIFS version 2 establish CIFS version 2 connections. Clients requesting a CIFS connection without specifying a version 2 connection establish CIFS version 1 connections.
- After SMB2 support is enabled on the storage server, some clients that support CIFS version 2 may continue to connect using CIFS version 1 connections until they have been restarted. This occurs because some clients cache connection type, and do not negotiate the connection type every time they connect. Clients that operate in this manner will continue to connect using CIFS version 1 until they have been restarted.

**Specifying the CIFS/SMB version used by the server**

To specify the maximum version of the CIFS/SMB protocol that the server will use, or view the current CIFS/SMB version configuration selected on the server, refer to the `cifs-max-supported-version` command.

**Configuring CIFS security**

The server integrates seamlessly into the existing domain and simplifies access control by performing all authentications against the existing domain user accounts.
Note: Only accounts that have been created in the domain or in a trusted domain can access the server.

When a user attempts to access a share, the server verifies appropriate permissions; once access is granted at this level, standard file and directory access permissions apply.

The server operates on a specific domain and can, optionally, join an Active Directory. It interacts with a domain controller (DC) in its domain to validate user credentials. The server supports Kerberos-based authentication to an Active Directory, as well as NTLM authentication (using pre-Windows 2000 protocols). In addition to users belonging to its domain, the server allows members of trusted domains to connect through CIFS.

The server automatically grants administrator privileges to domain administrators who have been authenticated by the DC. In addition, local administration privileges can be assigned, including backup operator privileges to selected groups (or users).

Assigning CIFS names

Windows clients access the server through configured CIFS names. Traditional Windows servers have a single host name; in environments where multiple Windows servers are being consolidated, the server can be configured with multiple CIFS names.

In order to appear as a unique server on a Windows network, the server will do the following for each configured CIFS name:

- Allow administration through the Microsoft Server Manager (NT 4) or Computer Management (Windows 2000, 2003, or 2008) administrative tools.
- If NetBIOS is enabled, register each CIFS name with the domain Master Browser so each name appears as a unique server in Network Neighborhood.
- Register each CIFS name with DDNS or WINS for proper host name resolution.
- Support up to 256 CIFS names per EVS.

Viewing CIFS Setup

Windows clients access the server through configured CIFS names. Traditional Windows servers have a single host name. In environments where multiple Windows servers are being consolidated, the server can be configured with multiple CIFS names.

In order to appear as a unique server on a Windows network, the server will do the following for each configured CIFS name:
• Allows administration through the Microsoft Server Manager (NT 4) or Computer Management (Windows XP, 2000, or 2003) administrative tools.
• Registers each CIFS name as a server with the domain Master Browser so each name appears as a unique server in Network Neighborhood.
• Registers each CIFS name with DDNS and WINS for proper host name resolution.
Procedure

1. Navigate to **File Services > CIFS Setup** to display the **CIFS Setup** page.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EVS</strong></td>
<td>Indicates the selected EVS. Click <strong>change</strong> to select another EVS.</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Currently configured security mode of the EVS.</td>
</tr>
<tr>
<td><strong>Security Mode</strong></td>
<td>The name of the NT domain in which the server resides. The domain is set when the first CIFS name is added.</td>
</tr>
<tr>
<td><strong>Domain Name</strong></td>
<td>The domain where the server is located.</td>
</tr>
<tr>
<td><strong>ADS Domain</strong></td>
<td>Whether DDNS is enabled or disabled.</td>
</tr>
<tr>
<td><strong>DDNS</strong></td>
<td>Whether DDNS is enabled or disabled.</td>
</tr>
<tr>
<td><strong>NetBIOS</strong></td>
<td>When NetBIOS is enabled, it allows NetBIOS and WINS use on this server. If this server communicates by name with computers that use earlier Windows versions, this setting is required. By default, the server is configured to use NetBIOS. Click <strong>disable</strong> to disable NetBIOS.</td>
</tr>
</tbody>
</table>

**Caution:** Before choosing to disable NetBIOS, verify that there is no need to use NetBIOS, WINS, or legacy NetBT-type applications for this network connection. If this server communicates only with computers that run Windows 2000, Windows XP, or Windows 2003, disabling...
<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>NetBIOS will be transparent and may even result in a performance benefit.</td>
</tr>
</tbody>
</table>

**Configured CIFS Server Names**

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIFS</td>
<td>Server Name The CIFS serving name is a list of CIFS names added to the selected EVS.</td>
</tr>
</tbody>
</table>
| Mode       | Displays the mode for each CIFS serving name. Mode defines the authentication protocol used to communicate with the Windows network clients and domain controllers. The mode can be:  
- ADS, meaning that the ADS style communication protocol (Kerberos) is used to communicate with the Windows clients and domain controllers.  
- NT4, meaning that the Windows NT 4 style communication protocol (NTLMSSP) is used to communicate with the Windows clients and domain controllers. |
| Disjoint   | A star under the column Disjoint indicates that the DNS and ADS domain names do not match. |
| add        | Opens the Add CIFS Server Names page, allowing you to add server names. |
| delete     | Deletes the selected CIFS server. |
| Reboot or Shut Down Server | Opens the Restart, Reboot and Shutdown page, which allows you to either restart or stop file serving, or to shut down or reboot a server, a cluster node, or an entire cluster. |
| File System Security | Opens the File System Security page, which displays all EVSs and the configured security mode. |

**Joining an Active Directory**

**Procedure**

1. Navigate to **Home > File Services > CIFS Setup** to display the CIFS Setup page.
2. Click **add** to display the **Add CIFS Server Names** page.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIFS Server Name</td>
<td>The computer name through which CIFS clients will access file services on the server. In an ADS domain, the maximum number of characters for the CIFS server name is 63. In an NT4 domain, the maximum number of characters for the CIFS server name is 15.</td>
</tr>
</tbody>
</table>
| Domain           | Indicates if the CIFS server is to be a part of an NT4 domain or an ADS domain, and allows you to specify the settings required to be a part of the domain.  
|                  |   - Before an NT4 name is added to the server, a computer account must exist in the NT Domain. Use Server Manager on the Domain Controller to create the computer account.  
|                  |   - When adding an ADS name to the server, the server will automatically create a computer account in the Active Directory for each added name. |

**Note:** This must be done for each NT4 CIFS name added.
<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NT4</td>
<td>Select the NT4 option to indicate that the CIFS server is to be a part of an NT4 domain.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Indicates that the CIFS server is to be part of an NT4 domain.</td>
</tr>
<tr>
<td>ADS</td>
<td>Indicates that the CIFS server is to be a part of an ADS domain.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of a domain controller in the Active Directory in which the server will be configured.</td>
</tr>
<tr>
<td>DC Admin User</td>
<td>A user account that is a member of the Domain Administrators group. This privilege is necessary to create a computer account in the Active Directory.</td>
</tr>
<tr>
<td>DC Admin Password</td>
<td>Password for the Domain Administrator user.</td>
</tr>
<tr>
<td>Folder</td>
<td>The folder in the Active Directory in which the computer account should be created. By default, the computer account will be created in the Computers folder.</td>
</tr>
<tr>
<td>DNS Suffix</td>
<td>Use this option only if you need to set a DNS suffix other than the Active Directory domain's primary DNS suffix. (For example, set this if you have a disjoint domain.)</td>
</tr>
<tr>
<td>OK</td>
<td>Saves configuration changes, and closes the page.</td>
</tr>
<tr>
<td>cancel</td>
<td>Closes the page without saving configuration changes.</td>
</tr>
</tbody>
</table>

3. Enter the name corresponding with the newly created computer account into the field labeled **CIFS Server Names**.

   - In an ADS domain, the maximum number of characters for the CIFS server name is 63.
   - In an NT4 domain, the maximum number of characters for the CIFS server name is 15.

4. If you are adding a server to an NT domain, complete the following steps. If you are joining an ADS domain, see step Joining an Active Directory on page 141.

   a. Select the **NT4** option.
   b. Enter the domain name.
   c. Click **OK** to return to the **CIFS Server** page.
   d. To create an NT 4 domain account, run Server Manager from a domain controller in the NT 4 Domain, and create a new Windows NT Workstation or Server account using the desired host name.

5. If you adding ADS domain, complete the following steps:

   a. Select the **ADS** option.
   b. In the **IP Address** field, specify the IP address of a domain controller in the Active Directory.
c. In the **DC Admin User** field, specify a user account that is a member of the Domain Administrators group. This privilege is necessary to create a computer account in the Active Directory. When specifying a user account from a trusted domain, the user account must be entered using the Kerberos format; that is, administrator@ADdomain.mycompany.com, not ADdomain\administrator.

d. In the **DC Admin Password** field, specify the password associated with the DC admin user name specified in step [Joining an Active Directory on page 141](#).

e. In the **Folder** field, specify the name of the folder in the Active Directory in which the computer account should be created. By default, the computer account will be created in the Computers folder.

f. Use the DNS Suffix option only if you need to set a domain name service suffix other than the AD domain's primary DNS suffix. For example, set this if you have a disjoint domain.

6. Click **OK**.

### Removing CIFS sever names

CIFS server names can be removed from the server’s configuration by deleting them from the list of configured CIFS server names. When ADS CIFS names are removed, the corresponding computer account in the Active Directory is also removed. Computer accounts in NT 4 Domains must be deleted manually through Server Manager.

---

**Caution:** CIFS Name Deletion Alert! At least one CIFS name must be configured on the server to support connections from Windows clients. As a result, if the last configured CIFS name is removed, Windows clients will no longer be able to access the server over CIFS.

---

**Note:** DNS entries do not de-register automatically after removing a CIFS server name, so the admin should delete the CIFS server name entry from DNS manually.

### Configuring local groups

In a Windows security domain, users and groups identify users (for example, vsmith) and groups of users (for example, software) on the network. Apart from the user-defined network group names (for example, software, finance, and test), Windows also supports a number of built-in or local groups with each providing various privileges and levels of access to the server on which they have been configured.
These groups exist on every Windows computer. They are not network groups, but are local to each computer. So, the user James may be granted Administrator privileges on one computer and not on another. Similarly in the server, the administrator can add users to any of these local groups, but only four of them are currently effective:

- **Root.** If a user is a member of the local Root group, the user bypasses all security checks, and can take ownership of any file in the file system.
- **Administrators.** If a user is a member of the local Administrators group, the user can take ownership of any file in the file system.
- **Backup Operators.** If a user is a member of the local Backup Operators group, the user bypasses all security checks, but cannot take ownership of a file in the file system. The privilege to bypass all security checks in the file system is required for accounts that run Backup Exec or perform virus scans. Virus scanner servers that are a part of the Backup Operators group can, however, take ownership of any file in the file system.
- **Forced Groups.** If a user is a member of the local Forced Groups group, when the user creates a file, the user’s defined primary group is overridden and the user account will be used to indicate the file creator’s name.

**Adding a local group or local group members**

**Procedure**

1. Navigate to Home > File Services > Local Groups to display the Local Groups page.
2. If necessary, click Change to select a different EVS security context or to select the global configuration. Changes made to local groups using this page apply only to the currently selected EVS security context.
   - If an EVS uses the Global configuration, any changes made to the global configuration settings will affect the EVS.
   - If an EVS uses an Individual security context, changes made to the global configuration settings will not affect the EVS. To manage local groups for an EVS that uses an individual security context, you must select the EVS’ individual security context to make changes, even if those settings are the same as the settings used by the global security context.
3. Click **add** to display the **Add Local Group** page.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group</strong></td>
<td></td>
</tr>
</tbody>
</table>
  • Select **Use existing local group** and then select from the list to add from an existing local group.  
  • Select **Add new local group** and then enter the name to add a new local group. |
| **Members** | Enter the member's user name and then click **add**. |
| **OK**      | Saves configuration changes, and closes the page. |
| **cancel**  | Closes the page without saving configuration changes. |

4. To add a new member to an existing local group, complete the following.  
   To add a new local group, see step **Adding a local group or local group members on page 145**.
   
   a. Select the **Use existing local group** option.
   b. Using the list of local groups, select the group to which you want to add a member.
   c. Enter the new member's user name in the Members field.
   d. Click **add**.
   e. Repeat steps **Adding a local group or local group members on page 145** and **Adding a local group or local group members on page 145** to add more members.
   f. Click **OK**.

5. To add a new local group, complete the following:
   a. Select the **Add new local group** option.
   b. Enter the new local group name in the **Members** field.
   c. If necessary, you can now enter group members for the new group. To enter members user names, enter each member's user name in the **Members** field.
   d. Click **add**.
Deleting a local group or local group members

Once created, group names may not be changed. To change a group name, you must delete the group, then create a new group, and add members to the new group.

Procedure

1. Navigate to **Home > File Services > Local Groups** to display the **Local Groups** page.
2. If necessary, click **Change** to select a different EVS security context or to select the global configuration. Changes made to local groups using this page apply only to the currently selected EVS security context.
   Deleting a local group is a two-stage process; you must delete all members of the group before you can delete the group itself.
3. Delete all members of the group:
   a. Fill the check box next to all members of the group you want to delete.
   b. Click **delete** to delete the selected group members.
   c. Click **OK** to confirm the deletion return to the **Local Groups** page.
4. Delete the local group:
   a. Fill the check box next to the group you want to delete.
   b. Click **delete** to delete the selected group.
   c. Click **OK** to confirm the deletion return to the **Local Groups** page.

Configuring CIFS shares

CIFS shares can be set up on mounted volumes. The server can support more than 1,000 shares. However, the exact limit of any share allocation depends on the server’s configuration.

Adding CIFS share

Procedure

1. Navigate to **Home > File Services > CIFS Share**.
2. Click **add** to display the **Add Share** page.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| Cluster Name Space/CNS or EVS/File System | Name of the currently selected context (either the cluster namespace context or an EVS local context) for which shares are displayed.  
- When the cluster namespace context is displayed, the list displays shares that link to the CNS tree. Users accessing those shares can go to the directories at or below that point in the CNS tree.  
- When a local EVS context and a file system are displayed, the list displays shares for file systems in the selected EVS. |
| Share Name                  | Name of the CIFS share.                                                                                                                                 |
| Comment                     | Additional information associated with the CIFS share. This information is often displayed to clients along with the share name.            |
| Path                        | The directory to which the CIFS share points. Users accessing the share will be able to access this directory, and any directories under it in the directory tree. To find a directory, click **browse**. |

**Note:** The **browse** button only exists if the path being created is the path in a file system, not a namespace.

Fill the **Create path if it does not exist** check box to create the path if it does not already exist.
<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Users</td>
<td>The maximum number of users who can be associated with the CIFS share. The default is unlimited.</td>
</tr>
<tr>
<td>Show Snapshots</td>
<td>• <strong>Show and Allow Access</strong>: Displays and allows access to snapshots. &lt;br&gt;• <strong>Hide and Allow Access</strong>: Hides snapshots, but still allows access to the hidden snapshots. &lt;br&gt;• <strong>Hide and Disable Access</strong>: Hides and disallows access to snapshots. Changes to this setting become effective when a CIFS client refreshes its folder view.</td>
</tr>
<tr>
<td>Cache Options</td>
<td>• <strong>Manual Local Caching for Documents</strong>: The Manual mode permits the user to specify individual files required for offline access. This operation guarantees a user can obtain access to the specified files whether online or offline. &lt;br&gt;• <strong>Automatic Local Caching for Documents</strong>: The Automatic mode is applied for all non-executable files on the entire share. When a user accesses any non-executable file in this share, it is made available to the user for offline access. This operation does not guarantee that a user can access all the non-executable files, because only those files that have been used at least once are cached. Automatic can also be defined for programs. &lt;br&gt;• <strong>Automatic Local Caching for Programs</strong>: The Automatic mode is applied for all executable files on the entire share. When a user accesses any executable file in this share, it is made available to the user for offline access. This operation does not guarantee that a user can access all the executable files, because only those executable files that have been used at least once are cached. Automatic can also be defined for documents. &lt;br&gt;• <strong>Local Caching Disabled</strong>: No caching of files or folders occurs.</td>
</tr>
<tr>
<td>Note:</td>
<td>The server supports Offline Files Access. This allows Windows 2000 and later clients to cache files that are commonly used from a network/file share. To use Offline Files, the client computer must be running Windows 2000 or later.</td>
</tr>
<tr>
<td>Transfer to Object</td>
<td>When a file system is recovered from a snapshot, one of the final steps is to import the CIFS shares found in the snapshot representing the selected version of the file system. Only those CIFS shares marked as transferable will be imported. Use the list to specify one of the following: &lt;br&gt;• <strong>Enable</strong>: CIFS shares will be transferred to recovered file systems. &lt;br&gt;• <strong>Disable</strong>: CIFS shares will not be transferred to recovered file systems. &lt;br&gt;• <strong>Use FS default</strong> (the default): When the target file system is brought online, CIFS shares will be transferred if Transfer Access Points During Object Replication is enabled for the file system.</td>
</tr>
<tr>
<td>Replication Target</td>
<td></td>
</tr>
<tr>
<td>Field/Item</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Access Configuration</td>
<td>IP addresses of the clients who can access the share (up to 2,000 characters allowed in this field). Refer to <strong>IP Address Configuration</strong> at the end of this table.</td>
</tr>
<tr>
<td>Follow Symbolic Links</td>
<td>Enables the following of symlinks for this share.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> As of release 12.2 of the Hitachi NAS Platform, clients using SMB2 or higher are able to follow relative symlinks to files on storage without the use of global symlinks.</td>
</tr>
<tr>
<td>Follow Global Symbolic Links</td>
<td>Enables CIFS clients to follow global (absolute) symlinks via Microsoft’s DFS mechanism for this share.</td>
</tr>
<tr>
<td>Force Filename to be Lowercase</td>
<td>Forces all filenames generated on this share to be lowercase. This is useful for interoperability of UNIX applications.</td>
</tr>
<tr>
<td>Enable ABE</td>
<td>By default, ABE is disabled for shares and on the server/cluster as a whole. Before enabling ABE for a share, you must make sure ABE is enabled for the server/cluster as a whole (the CLI command to enable ABE support is <code>fsm set disable-ABE-support false</code>). When enabled, ABE filters the contents of a CIFS share, so that only the files and directories for which a user has &quot;FileReadData&quot; or &quot;FileListDirectory&quot; rights are visible to the user (for example returned in a directory listing or considered by a wildcarded delete). Note that enabling ABE may have a negative impact on CIFS performance.</td>
</tr>
<tr>
<td>Enable Virus Scanning</td>
<td>If virus scanning is enabled and configured for the global context or for the EVS hosting the file system pointed to by the share then, when the share is created, virus scanning is enabled by default. If virus scanning is not enabled for the global context or for the EVS hosting the file system pointed to by the share then, when the share is created, virus scanning is not enabled by default, but you can enable it a per-EVS basis.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Virus scanning is set up on a per-EVS basis, or for all EVSs using the global configuration context, but cannot be set up on a per-server or per-cluster basis.</td>
</tr>
<tr>
<td>Share Permissions</td>
<td></td>
</tr>
<tr>
<td>Share Permissions List</td>
<td>By default, when a CIFS share is created, the group Everyone is added to the share permissions list.</td>
</tr>
<tr>
<td>User Home Directory Mapping</td>
<td>Used to specify how per-user home directories are created. The following options are available:</td>
</tr>
<tr>
<td>Mode</td>
<td>• <strong>Off.</strong> Disable the home directory feature for this share. Do not automatically create home directories on this share for users. This is the default.</td>
</tr>
<tr>
<td>Field/Item</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ADS</td>
<td>Create the user home directories based on the home directory information supplied by the Active Directory server for each user. If you select ADS, do not specify a Path.</td>
</tr>
<tr>
<td>User</td>
<td>Create the user’s home directory by converting the user’s Windows user name to lower case. (The user’s Windows domain name, if any, is ignored.) For example, a user <code>DOMAIN\John Smith</code> would result in a home directory of <code>john_smith</code>.</td>
</tr>
<tr>
<td>DomainAndUser</td>
<td>Create the user’s home directory by creating a directory named for the user’s Windows domain name, then converting the user’s Windows user name to lower case and creating a sub-directory by that name. For example, a user <code>DOMAIN\John Smith</code> would result in a home directory of “domain \john_smith”.</td>
</tr>
<tr>
<td>Unix</td>
<td>Create the user’s home directory by converting the user’s UNIX user name to lower case.</td>
</tr>
</tbody>
</table>

**Path**

Per-user home directories will be created in the specified Path, relative to the share root, which is specified without a leading \. If this field is left blank, user home directories will be created directly in the share root.

By default, only one share per file system can be configured with home directories. The cifs-home-directory command can be used to relax this restriction, in which case great care must be taken not to configure conflicting home directories.

For example, a share with a path of `\home1` and a share with a path of `\home2` would not cause a conflict, whatever home directory paths were configured. However, a share with a path of \ and a default home directory path would conflict with a share with a path of `\dir` and a default home directory path.

**OK**

Saves configuration changes, and closes the page.

**cancel**

Closes the page without saving configuration changes.

3. Click **change** to change the EVS/File System or Cluster Name Space (CNS) in which the CIFS share will reside.

4. Enter the Share Name. Clients will access the share through this name.

5. Type a comment that is meaningful to you or your users. This comment appears in Windows Explorer on client computers, and it is optional.

6. Type the Path to the directory being shared. Click **browse...** to help find an existing directory (this button only exists if the path being created is the path in a file system, not a name space). To create the path automatically when it does not already exist, click the **Create path if it does not exist** check box.

**Note:** Automatically created directories will be owned by the root user and group (UID:0 / GID:0) and will be accessible to all users, that is, the permissions are set to *rwxrwxrwx*. It is recommended that such directories are created via CIFS or NFS or that such directories are given the desired permissions explicitly after being created via this option.
7. To limit the number of users who can access the share simultaneously, enter the number of users in the **Max Users** field. By default, a share has unlimited access.

⚠️ **Note:** This only limits the number of users that can concurrently access a share. It does not provide security restrictions.

8. If snapshots are present and you want them to be visible to clients, fill the **Show snapshots** check box. If snapshots are not taken, or if you don't want clients to view snapshots, make sure this check box is empty.

9. To allow clients to traverse symbolic links, fill the **Follow Symbolic Links** check box.

10. To enable CIFS clients to follow global (absolute) symlinks via Microsoft's DFS mechanism for this share, fill the **Follow Global Symbolic Links** check box.

11. To force all characters to be lowercase when files and directories are created, fill the **Force Filenames to be Lowercase** check box.

12. To disable Virus Scanning for the share, clear the **Enable Virus Scanning** check box. The default setting will add this share to the server-wide Virus Scan.

⚠️ **Note:** Enable Virus Scanning is checked by default only if virus scanning is globally enabled.

13. To enable **ABE** (access based enumeration), fill the check box.

   ABE is disabled by default. When enabled, ABE filters the contents of a CIFS share, so that only the files and directories for which a user has FileReadData or FileListDirectory rights are visible to the user (for example returned in a directory listing or considered by a wildcard delete).

⚠️ **Note:** Enabling ABE may have a negative impact on CIFS performance.

14. To alter the caching option (Offline Files Access), select the desired new value from the Cache Options list.

15. To import the CIFS shares found in the snapshot representing the selected version of the file system, select the desired new value from the Transfer to Object Replication Target list. Only those CIFS shares marked as transferable will be imported.

16. In the **Access Configuration** field, specify the IP addresses of the clients who can access the share and the client's permissions for this share. The table outlines what to type in this field.
What to Type | Means
--- | ---
Blank or * | All clients can access the export.
Specific address or name. Examples: 10.168.20.2, client.dept.company.com | Only clients with the specified names or addresses can access the export.
A range of addresses using Classless Inter-Domain Routing (CIDR) notation. Example: 10.168.1.0/16 | Clients with addresses within the range can access the export.
Partial address or name using wildcards. Examples: 10.168.*.*.*, *.company.com | Clients with matching names or addresses can access the export.

17. Click **OK**.

**Displaying and modifying CIFS shares details**

**Procedure**

1. Navigate to **Home > File Services > CIFS Share**.
2. Fill the check box for the share to display or modify, and click **details**.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Name</td>
<td>Name of the currently selected context (either the cluster namespace context or an EVS local context) for which shares are displayed.</td>
</tr>
<tr>
<td>Space/CNS or EVS/File System</td>
<td>• When the cluster namespace context is displayed, the list displays shares that link to the CNS tree. Users accessing those shares can go to the directories at or below that point in the CNS tree.</td>
</tr>
<tr>
<td></td>
<td>• When a local EVS context and a file system are displayed, the list displays shares for file systems in the selected EVS.</td>
</tr>
<tr>
<td>change</td>
<td>Select a different context to display.</td>
</tr>
<tr>
<td>Share Name</td>
<td>Name of the CIFS share.</td>
</tr>
<tr>
<td>Comment</td>
<td>Additional information associated with the CIFS share. This information is often displayed to clients along with the share name.</td>
</tr>
<tr>
<td>Path</td>
<td>The directory to which the CIFS share points. Users accessing the share will be able to access this directory, and any directories under it in the directory tree. To find a directory, click <strong>browse</strong>.</td>
</tr>
</tbody>
</table>

**Note:** The **browse** button only exists if the path being created is the path in a file system, not a namespace.
<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fill the <strong>Create path if it does not exist</strong> check box to create the path if it does not already exist.</td>
<td>Max Users: The maximum number of users who can be associated with the CIFS share. The default is unlimited.</td>
</tr>
</tbody>
</table>
| Show Snapshots             | • **Show and Allow Access**: Displays and allows access to snapshots.  
• **Hide and Allow Access**: Hides snapshots, but still allows access to the hidden snapshots.  
• **Hide and Disable Access**: Hides and disallows access to snapshots.  
Changes to this setting become effective when a CIFS client refreshes its folder view. |
| Cache Options              | • **Manual Local Caching for Documents**: The Manual mode permits the user to specify individual files required for offline access. This operation guarantees a user can obtain access to the specified files whether online or offline.  
• **Automatic Local Caching for Documents**: The Automatic mode is applied for all non-executable files on the entire share. When a user accesses any non-executable file in this share, it is made available to the user for offline access. This operation does not guarantee that a user can access all the non-executable files, because only those files that have been used at least once are cached. Automatic can also be defined for programs.  
• **Automatic Local Caching for Programs**: The Automatic mode is applied for all executable files on the entire share. When a user accesses any executable file in this share, it is made available to the user for offline access. This operation does not guarantee that a user can access all the executable files, because only those executable files that have been used at least once are cached. Automatic can also be defined for documents.  
• **Local Caching Disabled**: No caching of files or folders occurs. |
| Note:                     | The server supports Offline Files Access. This allows Windows 2000 and later clients to cache files that are commonly used from a network/file share. To use Offline Files, the client computer must be running Windows 2000 or later. |
| Transfer to Object Replication Target | When a file system is recovered from a snapshot, one of the final steps is to import the CIFS shares found in the snapshot representing the selected version of the file system. Only those CIFS shares marked as transferable will be imported. Use the list to specify one of the following:  
• **Enable**: CIFS shares will be transferred to recovered file systems.  
• **Disable**: CIFS shares will not be transferred to recovered file systems.  
• **Use FS default** (the default): When the target file system is brought online, CIFS shares will be transferred if Transfer Access Points During Object Replication is enabled for the file system. |
<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Configuration</td>
<td>IP addresses of the clients who can access the share (up to 2,000 characters allowed in this field). Refer to <strong>IP Address Configuration</strong> at the end of this table.</td>
</tr>
<tr>
<td>Follow Symbolic Links</td>
<td>Enables the following of symlinks for this share.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> As of release 12.2 of the Hitachi NAS Platform, clients using SMB2 or higher are able to follow relative symlinks to files on storage without the use of global symlinks.</td>
</tr>
<tr>
<td>Follow Global Symbolic</td>
<td>Enables CIFS clients to follow global (absolute) symlinks via Microsoft’s DFS mechanism for this share.</td>
</tr>
<tr>
<td>Links</td>
<td></td>
</tr>
<tr>
<td>Force Filename to be</td>
<td>Forces all filenames generated on this share to be lowercase. This is useful for interoperability of UNIX applications.</td>
</tr>
<tr>
<td>Lowercase</td>
<td></td>
</tr>
<tr>
<td>Enable ABE</td>
<td>By default, ABE is disabled for shares and on the server/cluster as a whole. Before enabling ABE for a share, you must make sure ABE is enabled for the server/cluster as a whole (the CLI command to enable ABE support is <code>fsm set disable-ABE-support false</code>). When enabled, ABE filters the contents of a CIFS share, so that only the files and directories for which a user has “FileReadData” or “FileListDirectory” rights are visible to the user (for example returned in a directory listing or considered by a wildcarded delete). Note that enabling ABE may have a negative impact on CIFS performance.</td>
</tr>
<tr>
<td>Enable Virus Scanning</td>
<td>If virus scanning is enabled and configured for the global context or for the EVS hosting the file system pointed to by the share then, when the share is created, virus scanning is enabled by default. If virus scanning is not enabled for the global context or for the EVS hosting the file system pointed to by the share then, when the share is created, virus scanning is not enabled by default, but you can enable it a per-EVS basis.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Virus scanning is set up on a per-EVS basis, or for all EVSs using the global configuration context, but cannot be set up on a per-server or per-cluster basis.</td>
</tr>
<tr>
<td>Share Permissions</td>
<td></td>
</tr>
<tr>
<td>Share Permissions List</td>
<td>By default, when a CIFS share is created, the group Everyone is added to the share permissions list.</td>
</tr>
</tbody>
</table>
| User Home Directory Mapping | Used to specify how per-user home directories are created. The following options are available:  
• Off. Disable the home directory feature for this share. Do not automatically create home directories on this share for users. This is the default.                                                                                                                                                                                                 |
| Mode                    |                                                                                                                                                                                                                                                                                                                                             |
### Field/Item | Description
--- | ---
• ADS. Create the user home directories based on the home directory information supplied by the Active Directory server for each user. If you select ADS, do not specify a **Path**.
• **User**. Create the user’s home directory by converting the user’s Windows user name to lower case. (The user’s Windows domain name, if any, is ignored.) For example, a user `DOMAIN\John Smith` would result in a home directory of `john_smith`.
• **DomainAndUser**. Create the user’s home directory by creating a directory named for the user’s Windows domain name, then converting the user’s Windows user name to lower case and creating a sub-directory by that name. For example, a user `DOMAIN\John Smith` would result in a home directory of “domain\john_smith”.
• **Unix**. Create the user’s home directory by converting the user’s UNIX user name to lower case.

### Path
Per-user home directories will be created in the specified **Path**, relative to the share root, which is specified without a leading \\-. If this field is left blank, user home directories will be created directly in the share root.

By default, only one share per file system can be configured with home directories. The cifs-home-directory command can be used to relax this restriction, in which case great care must be taken not to configure conflicting home directories.

For example, a share with a path of `\home1` and a share with a path of `\home2` would not cause a conflict, whatever home directory paths were configured. However, a share with a path of `\` and a default home directory path would conflict with a share with a path of `\dir` and a default home directory path.

### OK
Saves configuration changes, and closes the page.

### cancel
Closes the page without saving configuration changes.

---

3. Modify the fields on this page as necessary.
4. Click **OK**.

**Controlling access to shares using qualifiers**

To specify which clients have access to a CIFS share, qualifiers can be appended to the IP addresses:

<table>
<thead>
<tr>
<th>Qualifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>read_write, readwrite, rw</td>
<td>Grants read/write access. This is the default setting.</td>
</tr>
<tr>
<td>read_only, readonly, ro</td>
<td>Grants the specified client read-only access to the CIFS share.</td>
</tr>
<tr>
<td>no_access, noaccess</td>
<td>Denies the specified client access to the CIFS share.</td>
</tr>
</tbody>
</table>

Some CIFS share qualifier examples are:
• **10.1.2.38**(ro)
  Grants read-only access to the client with an IP address of 10.1.2.38.
• **10.1.2.0/24**(ro)
  Grants read-only access to all clients whose IP address is within the range 10.1.2.0 to 10.1.2.255.
• **10.1.2.*(readonly)**
  Grants read-only access to all clients with an IP address beginning with 10.1.

The order in which the entries are specified is important. For example,

*(ro) 10.1.2.38(noaccess)*

in which the first line grants read-only access to all clients, and the second denies access to the specified client. However, the second line is redundant, as the first line matches all clients. These lines must be transposed to ensure access is denied to 10.1.2.38

### Controlling access to shares using permissions

Access to shares is restricted through a combination of share-level and file-level permissions. These permissions determine the extent to which users can view and modify the contents of the shared directory. When users request access to a share, their share-level permissions are checked first; if authorized to access the share, their file-level permissions are checked.

When the share-level permissions differ from the file-level permissions, the more restrictive permissions apply, as described in the following table, where [a] = “allowed” and [d] = “denied”:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Read</th>
<th>Change</th>
<th>Full</th>
</tr>
</thead>
<tbody>
<tr>
<td>View the names of files and subdirectories</td>
<td>a</td>
<td>a</td>
<td>a</td>
</tr>
<tr>
<td>Change to subdirectories of the shared directory</td>
<td>a</td>
<td>a</td>
<td>a</td>
</tr>
<tr>
<td>View data in files</td>
<td>a</td>
<td>a</td>
<td>a</td>
</tr>
<tr>
<td>Run applications</td>
<td>a</td>
<td>a</td>
<td>a</td>
</tr>
<tr>
<td>Add files and subdirectories</td>
<td>d</td>
<td>a</td>
<td>a</td>
</tr>
<tr>
<td>Change data in files</td>
<td>d</td>
<td>a</td>
<td>a</td>
</tr>
<tr>
<td>Delete files and subdirectories</td>
<td>d</td>
<td>a</td>
<td>a</td>
</tr>
<tr>
<td>Change permissions on files or subdirectories</td>
<td>d</td>
<td>d</td>
<td>a</td>
</tr>
<tr>
<td>Take ownership of files or subdirectories</td>
<td>d</td>
<td>d</td>
<td>a</td>
</tr>
</tbody>
</table>

When configuring access to a share, it is only possible to add users or groups that are:
• Known to domain controllers,
• Seen by the server on the network.

⚠️ **Note:** When a user is given access to a share, if the user has also a member of a group with a different access level, the more permissive level applies. For example, if a user is given *Read* access to a share, and that user also belongs to a group that has *Change* access to that same share, the user will have *Change* access to the share, because *Change* access is more permissive than *Read* access.

### Adding or changing CIFS share access permissions

**Procedure**

1. Navigate to **Home > File Services > CIFS Shares** to display the **CIFS Share** page.
2. Fill the check box next to the share to modify, and click **details** to display the **CIFS Share Details** page.
3. In the Share Permissions area of the **CIFS Share Details** page, click **change**.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New User/Group</td>
<td>Name for the new user or group.</td>
</tr>
<tr>
<td>Type</td>
<td>Displays a standardized identifier for the security group to which the user/group being added belongs. The value is set automatically, based on the well known security identifier for the user/group being added.</td>
</tr>
<tr>
<td>modify</td>
<td>Saves any modifications made to the user or group settings.</td>
</tr>
</tbody>
</table>

4. To add a new user or group, follow these steps. To change permissions for an existing user or group, see step **Adding or changing CIFS share access permissions on page 158**.
   a. Enter the name for the new user or group in the **New User/Group** field.
   b. Click the down arrow to add the new user or group.
   c. Select the new user/group, by clicking on the user/group name in the user/group list.
   d. Fill the **Allow** or **Deny** check boxes to set the appropriate permissions. If the Allow check box is filled for full control, the user/group can perform all actions.

5. To change user/group permissions:
   a. Select the user/group for which you want to change permissions.
b. Fill the **Allow** or **Deny** check boxes to set the appropriate permissions. If the Allow check box is filled for full control, the user/group can perform all actions.

c. Save changes by clicking **modify**.

### Offline file access modes

The server supports offline files access. This allows network clients to cache files that are commonly used from a network or file share. To use offline files, the client computer must be running Windows 2000 (or later). There are three different share caching modes (supporting all three modes of caching):

- **No Caching**: No caching of files or folders occurs.
- **Manual**: Allows user specification of individual files required for offline access. This operation guarantees a user can obtain access to the specified files whether online or offline.
- **Automatic**: Applies to the entire share. When a user accesses any file in this share, that file becomes available to that user for offline access. This operation does not guarantee a user can obtain access to the specified files, because only files that have been used at least once are cached. The Automatic mode can be defined for documents or programs.

### Backing up and restoring CIFS shares

When backing up and restoring CIFS Shares:

- All CIFS Shares in all EVSs are backed up (except those in the CNS tree).
- A CIFS Share backup file is saved as a `.txt` file. The backup file contains the file system name and the share name, as well as most of the information about the share, including the settings for: *Ensure Path Exists*, *Show Snapshots*, *Follow Symbolic Links*, *Force Filename to Lowercase*, *Virus Scanning*, *Cache Options*, and *Max Users*.

When you restore CIFS Shares from a backup file:

- The restore operation does not modify or overwrite currently existing shares that have the same name.
- With the exception noted above, all shares in the selected backup file are restored.

**Procedure**

1. Navigate to **Home > File Services > CIFS Shares** to display the **CIFS Shares** page.
2. Click **Backup & Recovery** to display the CIFS Shares Backup & Restore page,

![CIFS Shares Backup & Restore](image)

3. To back up: Click **backup**. In the browser, specify the name and location of the backup file, then click **OK** or **Save** (the buttons displayed and the method you use to save the backup file depend on the browser you use). A backup file name is suggested, but you can customize it. The suggested file name uses the syntax:

\[CIFS_SHARES\_date\_time.txt\]

where the following example illustrates the appropriate syntax:

\[CIFS\_SHARES\_Aug\_4\_2006\_11\_09\_22\_AM.txt\]

4. To restore: Click **restore**. In the browser, the backup text file (\[CIFS\_SHARES\_date\_time.txt\]) for the specific share(s) you want to restore, then click **Open**. When the CIFS Export Backup & Restore page displays the name and location of the selected file, click **Restore**.

### Using Windows server management

The Computer Management MMC tool, available for Windows 2000 or later, can perform share management tasks from any remote computer; for example:

- Viewing a list of all users currently connected to the system.
- Creating shares.
- Listing all shares on the system and the users connected to them.
- Disconnecting one or all of the users connected to the system or to a specific share.
- Closing one or all of the shared resources that are currently open.
- Viewing an event log.

**Note:** For older versions of Windows, the equivalent of this tool is provided by Server Manager.
Using the computer management tool

Note: The appearance of the screens depends on the operating system version.

To use the Computer Management tool:

Procedure

1. In the Windows interface, from Administrative Services, select \textit{Computer Management}; then right-click on \textit{Computer Management (Local)} to display a context menu, and select \textit{Connect to another computer}:

2. Optionally, select the domain from the drop-down \textit{Look in} field, then highlight a name or an IP address to use for file services on the server, and click \textit{OK}.

3. Click \textit{Event Viewer} to display the server’s event log:

4. On the event log window:
   - Click \textit{Shares} to list all of the shares. Some or all of the users can be disconnected from specific shares.
   - Click \textit{Sessions} to list all users currently connected to the system. Some or all of the users can be disconnected.
   - Click \textit{Open Files} to list all the open shared resources. Some or all of the shared resources can be closed.

Restoring a previous version of a file

CIFS clients can access previous versions of files stored on shares, as long as a snapshot containing the file/directory exists. A tab labeled Previous Versions is displayed on the \textit{Properties} page for files and folders for which previous versions are available from snapshots. The tab displays the list of the available previous versions and their corresponding times.

The tab provides a means to access directly the previous versions listed, or to restore from them.
Transferring files with FTP

This section explains how to set up File Transfer Protocol (FTP) so that users with FTP clients can access files and directories on the storage server.

- FTP protocol support
- Configuring FTP preferences
- FTP statistics
FTP protocol support

The server implements the file-serving functions of an FTP server. The server provides the file-serving functions required for:

- File manipulation.
- Directory manipulation.
- File access control (for example, permissions).

Prior to allowing FTP access to the system, the FTP service must be enabled. No license key is required for this protocol.

FTP statistics for the storage server (in 10-second time slices) are available for activity since the previous reboot or since the point when statistics were last reset.

Configuring FTP preferences

As part of the process of setting up FTP, choose a service for authenticating the passwords of the FTP users. Also, a timeout must be set with which to end FTP sessions that have been inactive.
Procedure

1. Navigate to Home > File Services > FTP Configuration to display the FTP Configuration page.

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| Password Authentication Services| The configured security mode determines what password authentication service methods can be used.  
  • NT  
    If selected, FTP users must log in with an NT domain user name and password, which is authenticated via a domain controller.  
  • NIS  
    If selected, FTP users must log in with a UNIX user name and password, which is authenticated via a NIS server in the configured NIS domain.  
  If both services are enabled, the FTP user will be authenticated against the configured NT domain first. If authentication fails, the server will attempt to authenticate the user against the configured NIS domain.  
  If both NT and NIS are not selected, then authentication will not be performed using these methods and only the anonymous user will be able to log in. |
| Anonymous User Permissions      | Specifies whether read-write is allowed for anonymous requests. Fill the ReadOnly check box to limit anonymous requests to read only. |
| Session Timeout                 | The number of minutes of inactivity after which to end an FTP session automatically (the Timeout). The valid range is from 15 to 14,400 minutes. |

2. In the Password Authentication Services area, fill the check box for NT or NIS.

   If operating in UNIX or Mixed security mode, both NT and NIS password authentication are supported. If both services are enabled, the FTP user will be authenticated against the configured NT domain first. If authentication fails, the server will attempt to authenticate the user against the configured NIS domain.

3. Enter the Session Timeout value.

Transferring files with FTP
4. Specify whether read-write is allowed for anonymous requests. Fill the **ReadOnly** check box to limit anonymous requests to read only.
5. Click **apply**.

**Displaying FTP users**

FTP users can be manually set up or display their details can be imported from a file.
Procedure

1. Navigate to Home > File Services > FTP Users to display the FTP Users page.

![FTP Users page](image)

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS / File System Label</td>
<td>This field displays the EVS and File System where the FTP users listed on the page have been configured.</td>
</tr>
<tr>
<td>change</td>
<td>Click the <strong>change</strong> button to select a different file system.</td>
</tr>
<tr>
<td>Filter</td>
<td>The filter button allows you to filter the users based on user Name or Path.</td>
</tr>
<tr>
<td>Name</td>
<td>This column displays the existing FTP users. Up to 5000 users can be listed, but the FTP user list displays a maximum of 20 users per page. Use filter to control the display of users.</td>
</tr>
<tr>
<td>File System</td>
<td>Shows the file system containing the FTP user’s initial directory path.</td>
</tr>
<tr>
<td>Path</td>
<td>Shows the path to the initial directory for the user after logging in over FTP.</td>
</tr>
<tr>
<td>details</td>
<td>Opens the <strong>FTP User Details</strong> page, allowing you to modify certain details about the selected user.</td>
</tr>
<tr>
<td>add</td>
<td>Opens the <strong>Add User</strong> page, allowing you to set up a new user.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes the selected user.</td>
</tr>
<tr>
<td>Import Users</td>
<td>Opens the <strong>Import FTP Users</strong> page, allowing you to set up new users by importing them from a file.</td>
</tr>
</tbody>
</table>
Adding an FTP user

Procedure

1. Navigate to Home > File Services > FTP Users to display the FTP Users page.
2. Click add to display the Add User page.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS / File System</td>
<td>Displays the selected file system.</td>
</tr>
<tr>
<td>change</td>
<td>To change the file system, click change to open the Select a File System page.</td>
</tr>
<tr>
<td>User Name</td>
<td>The name with which the user is to log in. To allow anonymous logins to the mount point, specify the user name as anonymous or ftp.</td>
</tr>
<tr>
<td>Initial Directory for the user</td>
<td>The directory in which the user starts when he or she logs in over FTP. Click browse to navigate to and insert the path.</td>
</tr>
<tr>
<td>Path Options</td>
<td>Create path if it does not exist check box creates the path automatically when it does not already exist.</td>
</tr>
<tr>
<td>OK</td>
<td>Saves configuration changes, and closes the page.</td>
</tr>
<tr>
<td>cancel</td>
<td>Closes the page without saving configuration changes.</td>
</tr>
</tbody>
</table>

Note: Automatically created directories will be owned by the root user and group (UID:0 / GID:0) and will be accessible to all users (that is, the permissions are set to rwxrwxrwx). It is recommended that such directories are created via CIFS or NFS, or that such directories are given the desired permissions explicitly after being created via this option.
3. Enter the user name. To allow anonymous logins to the mount point, specify the user name as anonymous or ftp. The password authentication service that you use determines whether users must log in with their NT domain name or UNIX user name.

4. In the Initial Directory for the user field, type the path to the directory in which the user starts when he or she logs in over FTP.

---

**Note:** Automatically created directories will be owned by the root user and group (UID:0 / GID:0) and will be accessible to all users (that is, the permissions are set to `rwxrwxrwx`). It is recommended that such directories are created using CIFS or NFS, or that such directories are given the desired permissions explicitly after being created with this option.

---

5. To create the path automatically when it does not already exist, select the **Create path if it does not exist** check box.

6. Click **OK**.

**Importing an FTP user**

**Procedure**

1. Navigate to **Home > File Services > FTP Users**.
2. Click **Import FTP Users** to display the **Import Ftp Users** page.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filename</td>
<td>The name of the file to import. Use the <strong>browse</strong> button to select the file.</td>
</tr>
<tr>
<td>Import</td>
<td>Click to import the file.</td>
</tr>
</tbody>
</table>

3. In the **Filename** field, enter the file name that contains the user details, or click **Browse** to search for the file name.

The user details in the import file have the following syntax:

```
user_name file_system initial_directory
```
Each entry must be separated by at least one space. If either the user_name or initial_directory contains spaces, the entry must be within double-quotes. For example:

```
carla Sales /Sales/Documents
miles Sales "/Sales/Sales Presentations"
john Marketing /Marketing
```

If you cannot be certain that the initial directory exists, you can create it automatically by specifying the option ENSURE_PATH_EXISTS on a separate line in the file. For example:

```
ENSURE_PATH_EXISTS true
carla Sales~/Sales/Documents
miles Sales "/Sales/Sales Presentations"
ENSURE_PATH_EXISTS false
john Marketing /Marketing
```

In the first instance of the ENSURE_PATH_EXISTS option, the true attribute turns on the option, and it applies to the two following entries until the option is turned off by the second instance of the option, with the attribute false. The default for the ENSURE_PATH_EXISTS option is true so that the initial directory is automatically created.

To insert a comment in the file, precede it with a hash character (#).

---

**Note:** Automatically created directories will be owned by the root user and group (UID:0 / GID:0) and will be accessible to all users (that is, the permissions are set to rwxrwxrwx). We recommend that such directories are created via CIFS or NFS, or that such directories are given the desired permissions explicitly after being created via this option.

4. Click **Import**.

**Modifying FTP users**

**Procedure**

1. Navigate to **Home > File Services > FTP Users**.
2. Fill the check box next to the user to display or modify, and click **details**.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File System</td>
<td>Displays the file system. Click <strong>change</strong> to select a different file system.</td>
</tr>
<tr>
<td>User Name</td>
<td>Displays the user name.</td>
</tr>
<tr>
<td>Initial Directory for the user</td>
<td>This directory is the location where the user starts after logging in over FTP. You can change the directory by typing the path to the new directory.</td>
</tr>
</tbody>
</table>
You can click the browse button to find the desired directory. This directory is the location where the user starts after logging in over FTP.

**Note:** Automatically created directories will be owned by the root user and group (UID:0 / GID:0) and will be accessible to all users (that is, the permissions are set to rwxrwxrwx). It is recommended that such directories are created via CIFS or NFS, or that such directories are given the desired permissions explicitly after being created by this option.

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path Options</td>
<td>Click the <strong>Create path if it does not exist</strong> check box to create the path automatically when it does not already exist.</td>
</tr>
<tr>
<td>OK</td>
<td>Saves configuration changes, and closes the page.</td>
</tr>
<tr>
<td>cancel</td>
<td>Closes the page without saving configuration changes.</td>
</tr>
</tbody>
</table>

3. Modify settings as needed:
   - In the File System field, you can click **change** to select a different file system.
   - In the Initial Directory for the user field, you can change the directory by typing the path to the new directory. You can click the browse button to find the desired directory. This directory is the location where the user starts after logging in over FTP.
   - In the **Path Options** box, you can fill the check box **Create path if it does not exist** to create the path automatically when it does not already exist.

4. Click **OK**.

### FTP statistics

FTP statistics for the storage server (in 10-second time slices) are available for activity since the previous reboot or since the point when statistics were last reset.

### Configuring FTP audit logging

FTP generates an audit log to keep track of user activity. The system will record the event when each time a user takes any of the following actions:
   - Logging in or out
   - Renaming or deleting a file
   - Retrieving, appending or storing a file
   - Creating or removing a directory

The system also records when a session timeout occurs.
Each log file is a tab-delimited text file containing one line per FTP event. Besides logging the date and time at which an event occurs, the system logs the user name and IP address of the client and a description of the executed command. The newest log file is called `ftp.log`, and the older files are called `ftpn.log` (the larger the value of $n$, the older the file).
Block-level access through iSCSI

The storage server supports iSCSI, the Internet Small Computer System Interface (iSCSI) protocol enables block-level data transfer between requesting applications and iSCSI target devices. Using Microsoft’s iSCSI Software Initiator (version 1.06 or later), Windows servers can view iSCSI targets as locally attached hard disks. Windows can create file systems on iSCSI targets, reading and writing data as if it were on a local disk. Window server applications, such as Microsoft Exchange and Microsoft SQL Server can operate using iSCSI targets as data repositories.

The server iSCSI implementation has attained the Designed for Windows Server™ 2003 certification from Microsoft. The Designed for Windows Server™ 2003 logo helps customers identify products that deliver a high quality computing experience with the Microsoft Windows Server 2003 operating syste.

- iSCSI support
- Configuring iSCSI
- Configuring iSCSI Logical Units
- Managing iSCSI logical units
- Configuring iSCSI security (mutual authentication)
- Accessing iSCSI storage
- Using Computer Manager to configure iSCSI storage
iSCSI support

To use iSCSI storage on the server, one or more iSCSI LUs (LUs) must be defined. iSCSI LUs are blocks of SCSI storage that are accessed through iSCSI targets. iSCSI targets can be found through an iSNS database or through a target portal. After an iSCSI target has been found, an Initiator running on a Windows server can access the LU as a “local disk” through its target. Security mechanisms can be used to prevent unauthorized access to iSCSI targets.

On the server, iSCSI LUs are just regular files residing on a file system. As a result, iSCSI benefits from file system management functions provided by the server, such as NVRAM logging, snapshots, and quotas.

The contents of the iSCSI LUs are managed on the Windows server. Where the server views the LUs as files containing raw data, Windows views each iSCSI target as a logical disk, and manages it as a file system volume (typically using NTFS). As a result, individual files inside of the iSCSI LUs can only be accessed from the Windows server. Server services, such as snapshots, only operate on entire NTFS volumes and not on individual files.
iSCSI MPIO

iSCSI MPIO (Multi-path Input/Output) uses redundant paths to create logical “paths” between the client and iSCSI storage. In the event that one or more of these components fails, causing the path to fail, multi-pathing logic uses an alternate path so that applications can still access their data.

For example, clients with more than one Ethernet connection can use logical paths to establish a multi-path connection to an iSCSI target on the server. Redundant paths mean that iSCSI sessions can continue uninterrupted in the event of the failure of a particular path. An iSCSI MPIO connection can also be used is to load-balance communication to boost performance.

If you intend to use an offload engine, make sure it is compatible with Microsoft multi-path and load-balancing.

iSCSI MPIO is supported by Microsoft iSCSI Initiator 2.0.
**iSCSI access statistics**

Statistics are available to monitor iSCSI activity since the server was last started or its statistics were reset. The statistics are updated every 10 seconds.

**iSCSI prerequisites**

To enable iSCSI capability:
- Enter an iSCSI license key.
- Enable the iSCSI service.

**Supported iSCSI initiators**

The server currently supports the following iSCSI initiators:
- Microsoft iSCSI Initiator version 1.06 (or later).
- Microsoft iSCSI Initiator version 2.05 (provides MPIO support).
- Linux iSCSI initiator versions 3.4.2, 3.6.2, 3.6.3, and 4.0.188.13 (available from the Linux iSCSI project on SourceForge).
- Solaris 10 U2 (64 bit) native initiator, iscsiadm v1.0.
- Macintosh (OS X 10.4 Tiger) ATTO Xtend SAN v3.10.
- Open iSCSI version 2.0.865.

**Note:** Other iSCSI initiators and/or versions of the initiators listed above may also work with the server, but have not been tested. Check with your Hitachi Data Systems representative for the latest list of supported iSCSI initiators.

**Offload engines**

The server currently supports the use of the Alacritech SES1001T and SES1001F offload engines when used with the Microsoft iSCSI initiator version 1.06 or later. Check with your Hitachi Data Systems representative for the latest list of supported offload engines.

**Configuring iSCSI**

In order to configure iSCSI on the server, the following information must be specified:
- iSNS servers
- iSCSI LUs
- iSCSI targets (including iSCSI domain)
- iSCSI initiators (if using mutual authentication)
Configuring iSNS

The Internet Storage Name Service (iSNS) is a network database of iSCSI initiators and targets. If configured, the server can add its list of targets to iSNS, which allows Initiators to easily find them on the network.

The iSNS server list can be managed through the iSNS page. The server registers its iSCSI targets with iSNS database when any of the following events occurs:

- A first iSNS server is added.
- An iSCSI target is added or deleted.
- The iSCSI service is started.
- The iSCSI domain is changed.
- A server IP address is added or removed.

Viewing iSNS servers

This page displays the list of configured iSNS servers. Each iSNS server is identified by its IP Address and the Port number through which the server will connect to the server.
Procedure

1. Navigate to Home > File Services > iSNS Servers to display the iSNS Servers page.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Lists the IP Address of the iSNS server.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number the NAS server uses to communicate with the iSNS server.</td>
</tr>
<tr>
<td>add</td>
<td>Click this button to add an iSNS server to the list.</td>
</tr>
<tr>
<td>delete</td>
<td>Saves configuration changes, and closes the page.</td>
</tr>
<tr>
<td>iSCSI Targets</td>
<td>Opens the iSCSI Targets window.</td>
</tr>
</tbody>
</table>

Configuring iSCSI Logical Units

Setting up iSCSI Logical Units

An iSCSI Logical Unit (LU) is a block of storage that can be accessed by iSCSI initiators as a locally attached hard disk. A LU is stored as a file on the server file system. Like any other data set on the file system, iSCSI LUs can be bound in size using the server’s size management tools, including virtual volumes and quotas. LUs are created with a specific initial size but can be expanded over time, as demand requires.

After a LU has been created and the iSCSI domain name has been set, an iSCSI Target must be created to allow access to the LU. A maximum of 32 LUs can be configured for each iSCSI Target.

Logical unit management

An iSCSI LU is a file within one of the server’s file systems. Such a file must have an .iscsi extension to identify it as an iSCSI LU. However, apart from
this extension there is no other way to determine that a file does indeed represent a LU.

---

**Note:** Hitachi Data Systems Support Center recommends that all iSCSI LUs are placed within a well-known directory, for example `/iscsi/`. This provides a single repository for the LUs in a known location.

---

**Logical unit security**

As LUs are files, they can be accessed over other protocols, such as CIFS and NFS. This renders LUs vulnerable to malicious users who can modify, rename, delete or otherwise affect them.

---

**Caution:** Hitachi Data Systems Support Center recommends setting sufficient security on either the LU file, the directory in which it resides, or both, to prevent unwanted accesses.

---

**Concurrent access to logical units**

The server's iSCSI implementation allows multiple initiators to connect to a single LU, which is necessary for applications and operating systems that support, or rely upon, concurrent file system access. However, concurrent access can be detrimental to a client machine when the client is unaware of other clients accessing the file system. For example:

- Simultaneous independent updates to the same files. Scenario: Two independent Microsoft Windows clients can connect to the same LU, containing an NTFS file system. Result: If allowed to simultaneously and independently modify data, metadata, and system files, conflicting disk updates will quickly corrupt the file system.

- Simultaneous access to separate partitions. Scenario: A LU contains two distinct NTFS partitions, with one Microsoft Windows client connected only to the first partition, and another connected only to the second partition. Result: Because a Microsoft iSCSI client will attempt to mount each partition it encounters on the LU, a Microsoft Windows client mounting an NTFS partition updates system files on all partitions; therefore, even though the two clients are accessing separate partitions within the LU, both will update system files on both partitions, causing conflicting system file updates, causing one or both of the clients to fail.

---

**Taking snapshots of logical units**

The contents of an iSCSI LU are controlled entirely by the client accessing it. The server cannot interpret the file systems or other data contained within a LU in any way. Therefore, the server has no knowledge of whether the data held within an iSCSI LU is in a consistent state. This introduces a potential problem when taking a snapshot of a LU.
For example, when a client creates a file, it must also insert the file name to the host directory. This means that more than one write is required to complete the operation. If the server takes a snapshot after the file object has been created, but before its name has been inserted into the directory, the file system contained within the snapshot will be inconsistent. If another client were to view the snapshot copy of the file system, it would see a file object without a name in a directory. This example provides only one possible scenario for snapshot inconsistency.

**Caution:** Hitachi Data Systems Support Center recommends that prior to taking a snapshot of an iSCSI LU, all applications should be brought into a known state. A database, for example, should be quiesced. Disconnecting the iSCSI initiators from the LUs undergoing snapshot is also recommended. This guarantees that all pending writes are sent to the LU before the snapshot is taken.

### Volume full conditions

Unexpected volume full conditions can occur with iSCSI LUs, as illustrated by the following two examples:

- **Directly Attached Disks.** When a client uses a directly attached disk, it can monitor the amount of available free space. If a partition contains no free space, the client can return a Volume Full condition. In this way, the client can ensure against file system corruption due to running out of disk space part way through an operation.

- **iSCSI LU.** By way of background, on iSCSI LUs with snapshots enabled, old data is preserved, not overwritten. Therefore, overwriting an area of a LU causes the server to allocate extra disk space, while using no extra disk space within the client’s partition, causing a Volume Full condition to occur, even when partitions within the LU contain free space. Under this scenario, a client may receive a Volume Full condition part-way through an operation, causing file system corruption. Although this corruption should be fixable, this situation should be avoided.

**Note:** Hitachi Data Systems Support Center recommends allocating sufficient disk space on the server to contain all iSCSI LUs and snapshots, as well as careful monitoring of free disk space.

### Managing iSCSI logical units

This section describes how to manage iSCSI logical units.
Viewing the properties of iSCSI Logical Units

Procedure

1. Navigate to Home > File Services > iSCSI Logical Units to display the iSCSI Logical Units page.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS/File System</td>
<td>Selector for EVS and File System where LUs reside, or where LUs can be created.</td>
</tr>
<tr>
<td>Alias</td>
<td>Name of the LU.</td>
</tr>
<tr>
<td>File System:Path</td>
<td>The file system and path for the LU.</td>
</tr>
</tbody>
</table>

⚠️ **Note:** LUs appear as regular files in server file systems.

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>Size of the LU, which may be up to the maximum file system size.</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates of the LU status, usually whether the LU is mounted.</td>
</tr>
</tbody>
</table>

⚠️ **Note:** The status will display Unmounted while a LU is being created asynchronously, and will then display Mounted once the creation has completed.
<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Used in Target</td>
<td>Displays the target.</td>
</tr>
<tr>
<td>mount</td>
<td>Select an unmounted LU and click mount to mount the LU.</td>
</tr>
<tr>
<td>unmount</td>
<td>Select a mounted LU and click unmount to unmount the LU.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes the selected iSCSI LUs.</td>
</tr>
<tr>
<td>add</td>
<td>Opens the Add iSCSI Logical Unit page where you can create a new iSCSI LU.</td>
</tr>
<tr>
<td>details</td>
<td>Opens the iSCSI Logical Unit Details page for the selected LU.</td>
</tr>
<tr>
<td>iSCSI Targets</td>
<td>Advances to the iSCSI Targets settings page.</td>
</tr>
<tr>
<td>iSCSI Initiator</td>
<td>Advances to the iSCSI Initiator Authentication settings page.</td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
</tr>
</tbody>
</table>
Adding iSCSI logical units

Procedure

1. Navigate to Home > File Services > iSCSI Logical Units and then click add to display the Add iSCSI Logical Units page:

![Add iSCSI Logical Unit](image)

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS/File System</td>
<td>Displays the Virtual Server and file system on which to create the Logical Unit.</td>
</tr>
<tr>
<td>File System Free Capacity: 995.85 GB</td>
<td></td>
</tr>
<tr>
<td>Alias</td>
<td>The name of the logical unit.</td>
</tr>
<tr>
<td>Path to File</td>
<td>The path where the logical unit resides. browse can be used to assist in finding the desired path of a predefined Logical Unit.</td>
</tr>
<tr>
<td>File Already Exists</td>
<td>Choose this option if the file already exists.</td>
</tr>
<tr>
<td>Create File</td>
<td>Choose this option if the file does not exist.</td>
</tr>
<tr>
<td>Size</td>
<td>The size of the Logical Unit. The size of the Logical Unit cannot exceed the amount of available free space on the configured file system. The maximum size of an iSCSI Logical Unit is 2 TB.</td>
</tr>
</tbody>
</table>
2. If necessary, change the EVS and/or file system. The EVS name displayed indicates the EVS and file system to which the LU will be added. Click **change** to select a different EVS or file system.

3. Specify the Logical Unit alias.
   In the **Alias** field, enter a name for the LU.

4. If the path to the file already exists, specify the path to the Logical Unit. When entering a path for an LU file that already exists, use the following procedure:
   a. Choose the file.
      Click **browse** to display a dialog that will allow you to select the file for the LU. Alternatively, you can enter the path name of the file (including the extension) and not use the browse button.
   b. Select the **File Already Exists** radio button.
   c. Optionally, add a comment.
      Using the comment field, you can provide descriptive information about the LU.
   d. Save the Logical Unit definition.
      Click **OK** to add the LU.

5. If the path to the file does not already exist, specify to create the path to the Logical Unit. There are several steps to complete when creating a new file for use as a LU:
   a. Choose the path for the file.
      Click **browse** to display a dialog that will allow you to select the directory for the LU file. The name of the file as well as the directory need to be specified. The file does not need an extension; iscsi is appended automatically. Alternatively, you can enter the file name and path (including the extension) and not use the browse button.
   b. Select the **Create File** radio button.
   c. Specify the logical unit size.
      Using the **Size** field and the drop-down list, specify the size of the LU file.
   d. Fill the **Create path to file if it does not exist** check box.
   e. Optionally, add a comment.
Using the **Comment** field, you can provide descriptive information about the LU.

**f.** Save the logical unit definition.

Click **OK** to add the LU.

### Modifying an iSCSI logical unit

**Procedure**

1. Navigate to **Home > File Services > iSCSI Logical Units**.
2. Fill the check box next to the iSCSI logical unit to modify and then click **details**.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS/File System</td>
<td>Displays the EVS and file system hosting the LU.</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates whether the LU is mounted or unmounted. It is possible to mount/unmount a LU while its underlying file system remains mounted. If the LU is not mounted, click <strong>mount</strong> to mount the LU. If the LU is mounted, click <strong>unmount</strong> to unmount the LU.</td>
</tr>
<tr>
<td></td>
<td>Filling the <strong>Ensure the underlying file system exists when mounting check box</strong> will ensure that the underlying file system exists when the LU is mounted.</td>
</tr>
<tr>
<td>Alias</td>
<td>Name of the LU. You can change this name.</td>
</tr>
<tr>
<td>Path to File</td>
<td>The complete file system path to the LU file.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> LUs appear as regular files in server file systems.</td>
</tr>
<tr>
<td>Size</td>
<td>Size of the LU.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The maximum size of a LU is 2 TB. This limit is imposed by the SCSI protocol.</td>
</tr>
<tr>
<td><strong>OK</strong></td>
<td>Saves configuration changes, and closes the page.</td>
</tr>
<tr>
<td><strong>cancel</strong></td>
<td>Closes the page without saving configuration changes.</td>
</tr>
<tr>
<td><strong>iSCSI Targets</strong></td>
<td>Takes you to the <strong>iSCSI Targets</strong> page, which allows you to add, modify, and delete iSCSI Targets.</td>
</tr>
</tbody>
</table>

3. Modify the fields as necessary.
4. Click **OK**.
Deleting an iSCSI logical unit

Procedure

1. Navigate to Home > File Services > iSCSI Logical Units to display the iSCSI Logical Units page.
2. Fill the check box next to the logical unit to delete and then click delete.
3. Click OK to confirm the deletion.

Backing up iSCSI logical units

Only a client connected to the LU through its Target can access and backup individual files and directories contained in the LU. LUs back up as normal files on a server file system.

Caution: If backing up the iSCSI LU from the server, ensure that the iSCSI initiators are disconnected, or make the backup from a snapshot.

To back up an iSCSI LU:

Procedure

1. Disconnect the iSCSI Initiator from the Target.
2. Unmount the iSCSI Logical Unit.
   To unmount the iSCSI LU, you can use the following CLI command:
   ```
   iscsi-lu unmount <name>
   ```
   Where `<name>` is the name of the iSCSI LU.
3. Back up the Logical Unit to a snapshot or backup device.
   For safety, you should either back up the iSCSI LU to a snapshot or to another backup device.
4. Mount the Logical Unit.
   To mount the iSCSI LU, you can use the following CLI command:
   ```
   iscsi-lu mount <name>
   ```
   Where `<name>` is the name of the iSCSI LU.
5. Reconnect to the iSCSI Target using the iSCSI Initiator.
6. If necessary, rescan disks.
   You may have to use Window's Computer Manager rescan disks to make the LU reappear to clients. S
**Restoring iSCSI logical units**

To ensure consistency of data on a LU, it may be necessary to restore it from a snapshot or a backup. To restore an iSCSI LU, perform the following steps:

**Procedure**

1. Disconnect the iSCSI Initiator from the Target.
2. Unmount the iSCSI logical unit.
   - Use the following CLI command: `iscsi-lu unmount <name>`, where `name` is the name of the LU
3. Restore the logical unit from a snapshot or backup.
4. Mount the iSCSI logical unit.
   - Use the following CLI command: `iscsi-lu mount <name>`, where `name` is the name of the LU.
5. Reconnect to the Target using the iSCSI Initiator.
6. If necessary, rescan disks in Computer Management.

**Setting up iSCSI targets**

An iSCSI target is a storage element accessible to iSCSI initiators. These targets appear to iSCSI initiators as different storage devices accessible over the network. The server supports a maximum of 32 iSCSI Targets per EVS and a maximum of 32 iSCSI sessions per Target.
Viewing the properties of iSCSI targets

Procedure

1. Navigate to Home > File Services > iSCSI Targets to display the iSCSI Targets page.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS</td>
<td>Select the EVS on which the target will be hosted.</td>
</tr>
<tr>
<td>change</td>
<td>Click to select a different EVS.</td>
</tr>
<tr>
<td>EVS iSCSI Domain</td>
<td>Displays the iSCSI Domain, which is the DNS domain used when creating unique qualified names for iSCSI targets.</td>
</tr>
<tr>
<td>Alias</td>
<td>Identifies the name of the target.</td>
</tr>
<tr>
<td>Comment</td>
<td>Additional information related to the target.</td>
</tr>
<tr>
<td>Globally Unique Name</td>
<td>The target’s name. The name is generated automatically by the server, and is unique across the globe.</td>
</tr>
<tr>
<td>details</td>
<td>Displays the details for the selected iSCSI target.</td>
</tr>
<tr>
<td>add</td>
<td>Advances to the Add iSCSI target page where you can add an iSCSI target.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes the selected iSCSI target.</td>
</tr>
<tr>
<td>iSCSI Logical Units</td>
<td>Advances to the iSCSI Logical Units settings page.</td>
</tr>
<tr>
<td>iSNS Servers</td>
<td>Advances to the iSNS Servers settings page.</td>
</tr>
<tr>
<td>iSCSI Initiator Authentication</td>
<td>Advances to the iSCSI Initiator Authentication settings page.</td>
</tr>
<tr>
<td>OK</td>
<td>Saves configuration changes, and closes the page.</td>
</tr>
</tbody>
</table>
### Adding iSCSI targets

**Procedure**

1. Navigate to **Home > File Services > iSCSI Targets** to display the **iSCSI Targets** page.

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cancel</td>
<td>Closes the page without saving configuration changes.</td>
</tr>
</tbody>
</table>
2. Click **add** to display the **Add iSCSI Target** page.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS</td>
<td>Select the EVS that will host the iSCSI Target. To view a different EVS, click the <strong>change</strong> button.</td>
</tr>
<tr>
<td><strong>change</strong></td>
<td>Clicking the change button opens the Select an EVS page.</td>
</tr>
<tr>
<td>iSCSI Domain</td>
<td>The DNS domain used when creating the Globally Unique Name of an iSCSI Target.</td>
</tr>
<tr>
<td>Alias</td>
<td>The name of the iSCSI Target.</td>
</tr>
<tr>
<td>Comment</td>
<td>Additional descriptive information about the Target.</td>
</tr>
<tr>
<td>Secret</td>
<td>The password used to secure the Target from any unauthorized access. The initiator authenticates against this password when connecting to the Target. The secret should be greater than or equal to 12 characters, but less than 17 characters, in length. Although the secret may be between 1-255 characters in length, some iSCSI initiators will refuse to connect if the secret contains less than 12 characters or more than 16 characters.</td>
</tr>
<tr>
<td>Enable Authentication</td>
<td>By default, the check box is not filled. Filling or clearing the checkbox enables or disables authentication. When authentication is disabled, initiators are permitted to connect</td>
</tr>
</tbody>
</table>
### Field/Item | Description
--- | ---
 | to the target and its logical units without needing to know the target's secret.
Access Configuration | Enter the desired access configuration parameters. Refer to the Access Configuration table for details on how to define the Access Configuration List.
Available Logical Units | The list of Logical Units available to assign an iSCSI Target.
Selected Logical Units | Enter a Logical Unit Number. The number can be any unique number between 0 and 255.
Logical Unit Number | Enter a Logical Unit Number. The number can be any unique number between 0 and 255.
OK | Click to add the iSCSI target.
cancel | Click to cancel and return to the iSCSI Targets page without modifying the target.

3. Specify the required information.
   a. The iSCSI Domain, Alias, Available LUs, and Logical Unit Numbers are required, all other fields are optional.
   b. Optionally, specify the Comment, Secret, and/or Access Configuration for the Target.

The following table provides syntax for the Access Configuration field:

<table>
<thead>
<tr>
<th>What to type</th>
<th>Means</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blank or *</td>
<td>All clients can access the target.</td>
</tr>
<tr>
<td>Specific address or name. Examples: 10.168.20.2, client.dept.company.com</td>
<td>Only clients with the specified names or addresses can access the target.</td>
</tr>
<tr>
<td>To deny access to a specific host, use the no_access or noaccess qualifier. For example, 10.1.2.38 (no_access) will deny access to the host with the IP address 10.1.2.38.</td>
<td></td>
</tr>
<tr>
<td>Partial address or name using wildcards. Examples: 10.168.<em>.</em>, *.company.com</td>
<td>Clients with matching names or addresses can access the target.</td>
</tr>
<tr>
<td>To deny access to a specific host, use the no_access or noaccess qualifier. For example, 10.1.2.38 (no_access) will deny access to the host with the IP address 10.1.2.38.</td>
<td></td>
</tr>
</tbody>
</table>

4. Click **OK**.
Adding a logical unit to an iSCSI target

Procedure

1. Navigate to Home > File Services > iSCSI Targets to display the iSCSI Targets page.
2. Fill the check box next to the target and then click details to display the iSCSI Target Details page.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS</td>
<td>Selector for EVS where LUs reside. Click change to switch to a different EVS.</td>
</tr>
<tr>
<td>EVS iSCSI Domain</td>
<td>Displays the iSCSI Domain, which is the DNS domain used when creating unique qualified names for iSCSI Targets.</td>
</tr>
<tr>
<td>Alias</td>
<td>Name of the iSCSI Target.</td>
</tr>
<tr>
<td>Comment</td>
<td>Additional information about the iSCSI Target.</td>
</tr>
<tr>
<td>Secret</td>
<td>Password used to secure the Target from any unauthorized access. The initiator authenticates against this password when connecting to the Target. The secret should be greater than or equal to 12 characters, but less than 17 characters, in length. Although the secret may be between 1-255 characters in length, some iSCSI initiators will refuse to connect if the secret contains less than 12 characters or more than 16 characters.</td>
</tr>
<tr>
<td>Enable Auth</td>
<td>Enable authentication of the iSCSI Target. By default, the check box is not filled. Filling or clearing the check box enables or disables authentication. When authentication is disabled, initiators are permitted to connect to the target and its LUs without needing to know the target’s secret.</td>
</tr>
<tr>
<td>Access Configuration</td>
<td>The access configuration parameters.</td>
</tr>
<tr>
<td>Available logical units</td>
<td>The list of LUs available for assignment to the iSCSI Target. This list includes all LUs on the EVS. Some of these LUs may already be assigned to other targets.</td>
</tr>
<tr>
<td>Selected LUN - LUN Name</td>
<td>The list of LUs selected to be part(s) of the iSCSI Target.</td>
</tr>
<tr>
<td>Field/Item</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Logical Unit Number</td>
<td>The number assigned to the LU (the LUN). Enter a Logical Unit Number in the range of 0-255.</td>
</tr>
<tr>
<td>OK</td>
<td>Saves configuration changes, and closes the page.</td>
</tr>
<tr>
<td>cancel</td>
<td>Closes the page without saving configuration changes.</td>
</tr>
</tbody>
</table>

3. Select a LU from the Available Logical Units list, specify a number (0-255) in the Logical Unit Number field, and click the right arrow to move the LU to the Selected Logical Units list.

**Note:** You should make sure that the LU is not already assigned to a target.

4. Click **OK**.

**Modifying the properties of an iSCSI Target**

**Procedure**

1. Navigate to **Home > File Services > iSCSI Targets** to display the **iSCSI Targets** page.
2. Fill the check box next to the target to modify and then click **details**.

The following table describes the fields on this page:

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS</td>
<td>Selector for EVS where LUs reside. Click change to switch to a different EVS.</td>
</tr>
<tr>
<td>EVS iSCSI Domain</td>
<td>Displays the iSCSI Domain, which is the DNS domain used when creating unique qualified names for iSCSI Targets.</td>
</tr>
<tr>
<td>Alias</td>
<td>Name of the iSCSI Target.</td>
</tr>
<tr>
<td>Comment</td>
<td>Additional information about the iSCSI Target.</td>
</tr>
<tr>
<td>Secret</td>
<td>Password used to secure the Target from any unauthorized access. The initiator authenticates against this password when connecting to the Target. The secret should be greater than or equal to 12 characters, but less than 17 characters, in length. Although the secret may be between 1-255 characters in length, some iSCSI initiators will refuse to connect if the secret contains less than 12 characters or more than 16 characters.</td>
</tr>
<tr>
<td>Field/Item</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable Auth</td>
<td>Enable authentication of the iSCSI Target. By default, the check box is not filled. Filling or clearing the check box enables or disables authentication. When authentication is disabled, initiators are permitted to connect to the target and its LUs without needing to know the target’s secret.</td>
</tr>
<tr>
<td>Access Configuration</td>
<td>The access configuration parameters.</td>
</tr>
<tr>
<td>Available logical units</td>
<td>The list of LUs available for assignment to the iSCSI Target. This list includes all LUs on the EVS. Some of these LUs may already be assigned to other targets.</td>
</tr>
<tr>
<td>Selected LUN - LUN Name</td>
<td>The list of LUs selected to be part(s) of the iSCSI Target.</td>
</tr>
<tr>
<td>Logical Unit Number</td>
<td>The number assigned to the LU (the LUN). Enter a Logical Unit Number in the range of 0-255.</td>
</tr>
<tr>
<td>OK</td>
<td>Saves configuration changes, and closes the page.</td>
</tr>
<tr>
<td>cancel</td>
<td>Closes the page without saving configuration changes.</td>
</tr>
</tbody>
</table>

3. The iSCSI Domain, Alias, Available LUs, and Logical Unit Numbers are required. Optionally, you can specify the Comment, Secret, and/or Access Configuration for the Target.

**Note:** Once set, the iSCSI Domain cannot be changed, but it will be overridden/replaced if you later specify a new iSCSI Target with a different iSCSI Domain in the same EVS. The most recently specified iSCSI Domain overrides all previously-specified iSCSI Domains set for all previously added iSCSI Targets in the EVS.

The following table describes what you can type in the Access Configuration field.

<table>
<thead>
<tr>
<th>What to type</th>
<th>Means</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blank or *</td>
<td>All clients can access the target.</td>
</tr>
<tr>
<td>Specific address or name. Examples: 10.168.20.2, client.dept.company.com</td>
<td>To deny access to a specific host, use the no_access or noaccess qualifier. For example, 10.1.2.38 (no_access) will deny access to the host with the IP address 10.1.2.38. Only clients with the specified names or addresses can access the target.</td>
</tr>
<tr>
<td>Partial address or name using wildcards. Examples: 10.168.<em>.</em>, *.company.com</td>
<td>To deny access to a specific host, use the no_access or noaccess qualifier. For example, Clients with matching names or addresses can access the target.</td>
</tr>
</tbody>
</table>
Deleting an iSCSI target

Procedure

1. Navigate to **Home > File Services > iSCSI Targets**.
2. Fill the check box next to the target to remove and then click delete.
3. To confirm the deletion, click OK.

Configuring iSCSI security (mutual authentication)

The storage server uses the Challenge Handshake Authentication Protocol (CHAP) to authenticate iSCSI initiators. CHAP requires a “shared secret” known by the initiator and the target. The server also supports mutual authentication where, in addition to the initiator authenticating against the target on the server, the server must also authenticate against the initiator.

To facilitate the mutual authentication process, the server must maintain a list of the initiators with which it can authenticate and the shared secret for each initiator.

Configuring the storage server for mutual authentication

To configure an EVS on the storage the server for iSCSI initiator mutual authentication:

Procedure

1. Navigate to **Home > File Services > iSCSI Initiator Authentication**.

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS</td>
<td>Displays the EVS on which to configure Initiator Authentication. Click change to select a different EVS.</td>
</tr>
<tr>
<td>Initiator Name</td>
<td>Identifies the initiator with a globally unique name.</td>
</tr>
<tr>
<td>Secret</td>
<td>Password used to secure the Initiator from any unauthorized access. The secret should be from 12 to 17 characters in length, but may be between 1-255 characters in length.</td>
</tr>
<tr>
<td>details</td>
<td>Click to display the iSCSI Initiator Details page for the selected initiator.</td>
</tr>
<tr>
<td>Check All</td>
<td>Click to fill the check box of all initiators in the list.</td>
</tr>
</tbody>
</table>
2. Make sure that the proper EVS is selected.
   Look at the EVS name listed at the top of the page. If this is not the EVS that you want the iSCSI initiator to connect with, click **change** and select the proper EVS.

3. Click **add** to add an iSCSI initiator.

4. Enter the iSCSI initiator name.
5. Enter the initiator secret (password).
6. Save the configuration.
Verify your settings, then click OK to save or cancel to return to the iSCSI Initiator Authentication page without adding the initiator.

Changing the storage server’s mutual authentication configuration

Once the storage server's iSCSI initiator configuration has been set up, you can either change an initiator's secret or delete it entirely.

Procedure

1. Navigate to Home > File Services > iSCSI Initiators.

<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EVS</td>
<td>Displays the EVS on which to configure Initiator Authentication. Click change to select a different EVS.</td>
</tr>
<tr>
<td>Initiator Name</td>
<td>Identifies the initiator with a globally unique name.</td>
</tr>
<tr>
<td>Secret</td>
<td>Password used to secure the Initiator from any unauthorized access. The secret should be from 12 to 17 characters in length, but may be between 1-255 characters in length.</td>
</tr>
<tr>
<td>details</td>
<td>Click to display the iSCSI Initiator Details page for the selected initiator.</td>
</tr>
<tr>
<td>Check All</td>
<td>Click to fill the check box of all initiators in the list.</td>
</tr>
<tr>
<td>Clear All</td>
<td>Click to empty the check box of all initiators in the list.</td>
</tr>
<tr>
<td>add</td>
<td>Click to display the Add iSCSI Initiator page.</td>
</tr>
<tr>
<td>delete</td>
<td>Click to delete the selected iSCSI initiator.</td>
</tr>
</tbody>
</table>

2. Make sure that the proper EVS is selected.

Look at the EVS name listed at the top of the page. If this is not the EVS that you want the iSCSI initiator to connect with, click change and select the proper EVS.

3. You can now either delete the initiator or change the initiator's secret.

   • To delete an iSCSI initiator:
     a. Fill the check box for the initiator you want to remove.
     b. Click delete to delete the selected initiator.

     A confirmation dialog appears, and you can click OK to delete the iSCSI Initiator, or cancel to return to the iSCSI Initiators page without deleting the Initiator.

   • To change the initiator's secret:
     a. Fill the check box for the initiator you want to change.
     b. Click details to display the iSCSI Initiator Details page for the selected initiator.
<table>
<thead>
<tr>
<th>Field/Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiator Name</td>
<td>The initiator’s globally unique name. This name is displayed in the Change Initiator node name dialog of the Microsoft iSCSI initiator.</td>
</tr>
<tr>
<td>Secret</td>
<td>The Secret for the Initiator. This is the secret which will be entered in the Chap Secret Setup dialog of the iSCSI Initiator. This secret is a password which is used to secure the Initiator from unauthorized access. The secret should be from 12 to 17 characters in length, but may be between 1-255 characters in length.</td>
</tr>
<tr>
<td>OK</td>
<td>If you have changed the initiator’s secret (password), click to update the configuration with the new secret.</td>
</tr>
<tr>
<td>cancel</td>
<td>Click to return to the iSCSI Initiator Authentication page without adding the initiator.</td>
</tr>
<tr>
<td>iSCSI Targets</td>
<td>Click to display the iSCSI Targets page.</td>
</tr>
</tbody>
</table>

c. In the Secret field, type the new secret.
   The secret should be from 12 to 17 characters in length, but may be between 1-255 characters in length.
d. Click OK to save the changed secret, or click cancel to return to the iSCSI Initiator Authentication page.

4. Click OK to save the changed secret, or click cancel to return to the iSCSI Initiator Authentication page.
5. Click details to display the iSCSI Initiator Details page.

**Configuring the Microsoft iSCSI initiator for mutual authentication**

---

**Note:**
- For the latest version of Microsoft iSCSI Software Initiator, visit: http://www.microsoft.com/.
- The visible screens depend on the operating system version.

To configure the Microsoft iSCSI Initiator for mutual authentication:

**Procedure**

1. Navigate to the iSCSI Initiator Properties on your Windows system:
   a. Start the Microsoft iSCSI Initiator.
   b. Open the iSCSI Initiator Properties dialog.
   c. Select the General tab.
   d. Click Secret to display the CHAP Secret Setup dialog.
Note: The shared secret is used to authenticate an initiator with a server, and it should be different from the secret specified when setting up the target.

e. Enter a secret.
   In the field, enter the secret which allows the target to authenticate with initiators when performing mutual CHAP.
f. Click OK to save the secret and return to the General tab of the iSCSI Initiator Properties dialog.

2. If necessary, change the initiator node name.
   If necessary, you can change the initiator node name.
a. Click Change to display the Initiator Node Name Change dialog.
b. Change the name as necessary.
   The initiator node name is the name which should be used as the initiator name on the storage server's iSCSI Initiator Authentication page (Home > File Services > iSCSI Initiators).

3. Verify the configuration settings.
4. Click OK to save the changes.

**Accessing iSCSI storage**

iSCSI LUs can be accessed through their targets using the Microsoft iSCSI Initiator. Discovered through iSNS or through the target portal, all iSCSI targets that are available will be displayed as available targets by the Initiator.

Note: Microsoft currently only supports creating a Basic Disk on an iSCSI LU. To ensure data integrity, do not create a dynamic disk. For more information, refer to the Microsoft iSCSI Initiator User Guide.

If its underlying volume is mounted read-only by the storage server, or if it is a snapshot copy of another LU, an iSCSI LU will also be read-only. In turn, if a LU is read-only, then any file systems contained within it will also be read-only. Clients accessing such read-only file systems will not be able to change any part of them, including file data, metadata or system files.

Although they can mount read-only FAT and FAT32 file systems, Microsoft Windows 2000 clients cannot mount read-only NTFS file systems. Microsoft Windows 2003 clients can mount read-only FAT, FAT32 and NTFS file systems. Therefore, if Microsoft Windows clients are required to access read-only NTFS file systems over iSCSI, Microsoft Windows 2003 must be used.
Using iSNS to find iSCSI targets

Using iSNS is the easiest way to find iSCSI targets on the network. If the network is configured with an iSNS server, configure the Microsoft iSCSI initiator to use iSNS. To add an iSNS server:

⚠️ Note: The appearance of the screens depend on the operating system version.

Procedure

1. Navigate to the iSCSI Initiator Properties on your Windows system.
2. Open the iSCSI Initiator Properties dialog.
3. Select the Discovery tab.
4. In the iSNS Servers area, click Add to display the Add iSNS Server dialog.
5. Enter the IP address or DNS host name for the iSNS server.
6. Click OK to save the IP address or host name and return to the Discovery tab of the iSCSI Initiator Properties dialog.
7. If necessary, add another iSNS server.

⚠️ Note: After the iSNS servers have been added, all available iSCSI targets that have been registered in iSNS will appear as available targets.

8. Save your changes.

Verify your settings, and then click OK to save the iSNS servers or Cancel to decline.

Using target portals to find iSCSI targets

If there are no iSNS servers on the network, iSCSI targets can be found through the use of target portals. Add the file services IP address of the EVS to the target portals list to find targets associated with that server or EVS.

⚠️ Note: The appearance of the screens depend on the operating system version.

Procedure

1. Navigate to the iSCSI Initiator Properties on your Windows system.
2. Open the iSCSI Initiator Properties dialog.
3. Select the Discovery tab.
4. In the Target Portals area, click Add to display the Add Target Portal dialog.
5. Enter the file services IP address of the EVS.
6. Click **OK** to save the IP address and return to the **Discovery** tab of the **iSCSI Initiator Properties** dialog.
7. If necessary, add another target portal.
8. Save your changes.

   Verify your settings, then click **OK** to save the list of target portals or **Cancel** to decline.

**Accessing available iSCSI targets**

To access an available iSCSI Target:

---

**Note:** The appearance of the screens depends on the operating system version.

**Procedure**

1. Navigate to the iSCSI Initiator Properties on your Windows system.
2. Open the **iSCSI Initiator Properties** dialog.
3. Select the **Targets** tab.
4. Select a target.
5. Click **Log On** to display the **Log On to Target** dialog.

---

**Note:** Each logon starts an iSCSI session, and a maximum of 32 iSCSI sessions are allowed per Target.

6. Click **OK** to log on to the target.
7. If authentication is enabled on the target, click **Advanced...** to open the **General** tab in the **Advanced Settings** dialog.
   
   1. Fill the **CHAP logon information** checkbox and enter the **Target secret** (the password configured when the iSCSI target was created).
   
   2. If mutual authentication has been configured, fill the **Perform mutual authentication** checkbox.
   
   3. Click **OK** to save the settings and return to the **Log On to Target** dialog.

   If multi-pathing is supported by the Microsoft iSCSI initiator, and you want to use multiple paths to the target, fill the **Enable multi-path** checkbox.

   To create multiple paths to the target, you must later start another session to the target.
9. Establish the connection.

   Click **OK** to establish the connection to the selected target.
Verifying an active connection

After the connection has been established, you can view any details about the newly established connection.

⚠️ Note: The appearance of the screen depends on the operating system version.

Procedure

1. Navigate to the iSCSI Initiator Properties on your Windows system.
2. Open the iSCSI Initiator Properties dialog.
3. Select the Targets tab.
4. Look at the Status column for the target.
   The Status column for the target should display "Connected."

Terminating an active connection

After the connection has been established, you can terminate the connection if necessary. To end the connection:

⚠️ Note: The appearance of the screens depends on the operating system version.

Procedure

1. Navigate to the iSCSI Initiator Properties on your Windows system.
2. Open the iSCSI Initiator Properties dialog.
3. Select the Targets tab.
4. Select the target with the connection you want to end.
5. Click Details to display the Target Properties dialog.
6. Select the session to terminate.
   In the list of sessions, select the identifier for the session you want to end.
7. Click Log off... to terminate the session.
   The initiator will attempt to close the iSCSI session if there are no applications currently using the devices.

Using Computer Manager to configure iSCSI storage

The iSCSI “local disk” must be configured through Windows Disk Management tools, and Microsoft recommends that:
- If the LU is smaller than 2 Tb, it should be configured as a Basic Disk.
- If the LU is larger than 2 Tb, it should be configured as a GPT Disk.
Once the disk is configured, use the Windows **Disk Management** tools to create and format a partition on the disk. For information and instructions on using the Windows **Disk Management** tools, refer to the online help of the operating system on your Windows computer.
Using Hitachi Dynamic Provisioning

You can use Hitachi Dynamic Provisioning (HDP) software to improve your storage utilization. The HDP software uses storage-based virtualization layered on top of RAID technology (RAID on RAID) to enable virtual LUNs (dynamically provisioned volumes, DP-Vols) to draw space from multiple pool volumes. This aggregated space widens the storage bottleneck by distributing the I/O to more disks. The greater distribution insulates the server from the realities of the pool volumes (small capacities of individual disks).

If you are using HDP, see the Hitachi NAS Platform Storage Pool and HDP Best Practices (MK-92HNAS048) for recommendations.

- **HDP high-level process**
- **Understanding HDP thin provisioning**
- **Understanding how HDP works with HNAS**
**HDP high-level process**

The following flow chart shows the high-level process for provisioning storage with HDP:

![Flow chart showing the high-level process for HDP provisioning]

**Figure 8-1 High-level process for HDP provisioning**

**Understanding HDP thin provisioning**

Dynamic provisioning allows storage to be allocated to an application without it actually being physically mapped until it is used. It also decouples the provisioning of storage to an application from the physical addition of storage capacity to the storage system. Thin provisioned HDP allows the total capacity of the DP-Vols in a pool to exceed the capacity of the volumes in the pool. For example, the pool volumes can total 30TiB, and the DP-Vols can total 80TiB. The server interprets the capacity as 80TiB of storage.
**Note:** Hitachi Data Systems strongly recommends that you always use thin provisioning with HDP.

The HDP software reads the real space in a pool. When you create or expand file systems using thin-provisioning with HDP, the server uses no more space than the space the pool vols provide. This also allows for file system creation and expansion to now fail safely.

HDP allocates pages of real disk space as the server writes data. The server can write anywhere on any DP-Vol, but not everywhere, meaning that you cannot exceed the amount of real disk space provided by the pool volumes.

### Understanding how HDP works with HNAS

Using HDP with HNAS provides many benefits.

HDP with HNAS provides the following benefits:

- Improves performance by striping I/O across all available disks
- Supports scalability of larger LUs (typically up to 64TiB)
- Eliminates *span-expand* and dynamic read balancing (DRB), and their limitations. When HDP thin provisioning is used, a pool can be expanded in small increments any number of times. However, if you expand a storage pool, make the increments as large as the initial size of the storage pool to avoid performance problems.
- File system creation or expansion still fails safely, even in the presence of thinly provisioned pools

To fully realize those benefits, see the HDP configuration guidelines in the *Storage Subsystem User Administrator Guide*.

Some limitations with HDP thin provisioning and HNAS exist. Consider the following:

- Some storage arrays and systems do not over-commit by more than a factor of ten to one.
- The amount of memory the storage needs for HDP is proportional to the size of the (large, virtual) DP-Vols, not the (smaller, real) pool volumes. Therefore, massive over-commitment causes the storage to prematurely run out of memory.
- Enterprise storage uses separate boards called *shared memory*, so consider over-committing by 2:1 or 3:1, rather than 100:1.