HITACHI
Inspire the Next

Hitachi Unified Storage File Module

Snapshot Administration Guide

Release 12.1

Hitachi Data Systems

MK-92USF008-05

Hitachi Data Systems products and services can be ordered only under the terms and conditions of Hitachi Data Systems' applicable agreements. The use of Hitachi Data Systems products is governed by the terms of your agreements with Hitachi Data Systems.

Hitachi is a registered trademark of Hitachi, Ltd., in the United States and other countries. Hitachi Data Systems is a registered trademark and service mark of Hitachi, Ltd., in the United States and other countries.

Archivas, Dynamic Provisioning, Essential NAS Platform, HiCommand, Hi-Track, ShadowImage, Tagmaserve, Tagmasoft, Tagmasolve, Tagmastore, TrueCopy, Universal Star Network, and Universal Storage Platform are registered trademarks of Hitachi Data Systems Corporation.

AIX, AS/400, DB2, Domino, DS8000, Enterprise Storage Server, ESCON, FICON, FlashCopy, IBM, Lotus, OS/390, RS6000, S/390, System z9, System z10, Tivoli, VM/ESA, z/OS, z9, zSeries, z/VM, z/VSE are registered trademarks and DS6000, MVS, and z10 are trademarks of International Business Machines Corporation.

All other trademarks, service marks, and company names in this document or website are properties of their respective owners.

Microsoft product screen shots are reprinted with permission from Microsoft Corporation.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/). Some parts of ADC use open source code from Network Appliance, Inc. and Traakan, Inc.

Part of the software embedded in this product is gSOAP software. Portions created by gSOAP are copyright 2001-2009 Robert A. Van Engelen, Genivia Inc. All rights reserved. The software in this product was in part provided by Genivia Inc. and any express or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the author be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

The product described in this guide may be protected by one or more U.S. patents, foreign patents, or pending applications.

Notice of Export Controls

Export of technical data contained in this document may require an export license from the United States government and/or the government of Japan. Contact the Hitachi Data Systems Legal Department for any export compliance questions.

Contents

Preface

In PDF format, this guide provides information about configuring the server to take and manage snapshots.

Document Revision Level

Revision	Date	Description
MK-92USF008-00	July 2012	First publication
MK-92USF008-01	September 2012	Revision 1, replaces and supersedes MK-92USF008-00.
MK-92USF008-02	June 2013	Revision 2, replaces and supersedes MK-92USF008-01.
MK-92USF008-03	November 2013	Revision 3, replaces and supersedes MK-92USF008-02.
MK-92USF008-04	April 2014	Revision 4, replaces and supersedes MK-92USF008-03.
MK-92USF008-05	September 2014	Revision 4, replaces and supersedes MK-92USF008-04.

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-92USF002)—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-92USF007)—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-92USF011)—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-92USF003)—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-92USF004)—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-92USF005)—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-92USF006)—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-92USF008)—In PDF format, this guide provides information about configuring the server to take and manage snapshots.
- *Replication and Disaster Recovery Administration Guide* (MK-92USF009)—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-92USF010)—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-92USF012)—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 Unified Storage File Module 3080 3090 G2 Hardware Reference* (MK-92USF001)—Provides an overview of the second-generation server hardware, describes how to resolve any problems, and replace potentially faulty parts.
- *Hitachi Unified Storage File Module 4000 Hardware Reference* (MK-92HNAS030) —Provides an overview of the Hitachi Unified Storage File Module 4000 server hardware, describes how to resolve any problems, and how to replace potentially faulty components.

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 Best Practices Guide for NFS with VMware vSphere* (MK-92HNAS028)—This document covers VMware best practices specific to HDS HNAS storage.
- *Hitachi NAS Platform Deduplication Best Practice* (MK-92HNAS031) —This document provides best practices and guidelines for using HNAS Deduplication.
- *Hitachi NAS Platform Best Practices for Tiered File Systems* (MK-92HNAS038) —This document describes the Hitachi NAS Platform feature that automatically and intelligently separates data and metadata onto different Tiers of storage called Tiered File Systems (TFS).
- *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).

1

Snapshots

For users whose data availability cannot be disrupted by management functions such as system backup and data recovery, snapshots create near-instantaneous, read-only images of an entire file system at a specific point in time. Snapshots safely create backups from a running system, allowing users to easily restore lost files without having to retrieve the data from backup media, such as tape.

Snapshots capture a moment in time for a live file system. They contain only those blocks that have changed since the snapshot was created, such that the disk space occupied by a snapshot is a fraction of that used by the original file system. However, over time, the space occupied by a snapshot grows, as the live file system continues to change.

Snapshots solve the problem of maintaining consistency within a backup; specifically, during a system backup, users continue to modify its component files, resulting in backup copies that may not provide a consistent set. Since a snapshot provides a frozen image of the file system, a backup copy of a snapshot (rather than of the live file system) provides a usable, consistent backup that appears to a network user like a directory tree. Users with appropriate access rights can retrieve the files and directories that it contains through CIFS, NFS, FTP, or NDMP.

- ☐ Snapshots and the volume shadow copy service (VSS)
- ☐ Latest snapshot
- ☐ Quick snapshot restore
- ☐ Accessing snapshots through NFS exports and CIFS shares

Snapshots and the volume shadow copy service (VSS)

Snapshots of storage attached to the storage server may be initiated by Microsoft's Volume Shadow Copy Service (VSS). VSS is available on servers running Windows Server 2003 or 2008, and it provides a coordination point for enabling consistent backups of online storage. Snapshots initiated by VSS are exported as iSCSI LUNs.

Storage writers (for example MS Exchange or a backup application) first register with VSS. A VSS credential is saved on both the VSS host and the NAS server. The server address and port number are saved along with the credential. This means that if the NAS server's VSS management port setting is changed, any existing VSS credentials for that server must be removed and new credentials must be created. If a DNS name is used for a NAS server, then changes to the server's IP address alone will not require removing and recreating the credential.

Note: A VSS credential has limited rights on the server: it can only be used to perform VSS-related operations using the VSS management interface. In particular it cannot be used to gain access to the normal NAS server management console, either locally or remotely.

Then, when a backup application wishes to back up a piece of storage (a "volume"):

1. The backup application requests that VSS take the snapshot.
2. VSS requests that all registered writers flush their data to make sure that all of their on-disk data files are in a consistent state.
3. After the writers report completion of this step, VSS takes the snapshot. When a VSS initiated snapshot is taken of a file system, the snapshot is added to the iSCSI target as one or more iSCSI LUs (one iSCSI LU is added for each source LU supplied to VSS). The snapshot LUs are then visible to the VSS host (the system on which the VSS Hardware Provider is installed) and are used as the backup source.

Note: If a VSS snapshot request contains LUs on different file systems, then only one snapshot will be created for all the LUs in each file system. However, copies of each requested LU are always created and made visible to the VSS host by the NAS server.

4. VSS then returns a pointer to the snapshot to the backup application so that the backup application can back up a stable view of the storage (the snapshot).
5. After the backup is completed, the backup application notifies VSS so that the snapshot may be deleted.

For non-persistent snapshots, once the backup is complete, the snapshot LUs are removed from the target and the VSS initiated snapshot(s) are deleted.

Persistent snapshots should be deleted via the backup application whenever possible. Although it is possible to delete a VSS initiated snapshot via the CLI or Web Manager, care must be taken to ensure that a backup application is not active and an iSCSI host is not bound to the snapshot's LU(s). Properly deleting a snapshot will also result in the snapshot LUs being removed from the target.

Note: Using the CLI or Web Manager to delete VSS initiated snapshots or to remove the snapshot LUs from their associated iSCSI target will result in the unexpected removal of a disk from the VSS host system, and can cause the VSS host to crash.

VSS may also be used to take "point in time" copies for later reference. The process is similar, except in this case no automatic deletion of the snapshot is performed by VSS. The storage server supports this mechanism by means of a VSS "hardware provider," a DLL which registers with VSS in order to support snapshots of volumes attached to a storage server.

Note: Snapshots initiated by the VSS service only contain images of iSCSI LUNs attached to the storage server. Non-iSCSI volumes attached to the storage server are not included in snapshots initiated by VSS.

For information about configuring VSS access to the storage server, see Configuring the NAS server for VSS shadow copies on page 24.

Latest snapshot

The storage server provides a file system view that can be used to access the *latest snapshot* for a file system. This view automatically changes as new snapshots are taken, but is not affected by changes in the live file system. The latest snapshot is the most recent snapshot for the file system, and is accessible through `.snapshot/.latest` (or `~snapshot/.latest`). The latest snapshot can be exported to NFS clients with the path `/.snapshot/.latest`. Latest snapshots can also be shared to CIFS clients. When accessing files via the latest snapshot, NFS operations do not use auto inquiry or auto response.

Note: The `.latest` (`~latest`) file designation is a hidden snapshot directory and does not show up in directory listings.

Quick snapshot restore

Quick Snapshot Restore (QSR) is a licensed feature for rolling back one or more files to a previous version of a snapshot. For more information about this command line procedure, open the CLI and run man snapshot, or refer to the *Command Line Reference*.

If a file has been moved, renamed or hard linked since the snapshot was taken, Quick Snapshot Restore may report that the file cannot be restored. If the file cannot be restored this way, it must be copied from the snapshot to the live file system normally.

Accessing snapshots through NFS exports and CIFS shares

NFS exports and CIFS shares can easily access snapshots, so that users can restore older versions of files without intervention.

- The root directory in any NFS export contains a `.snapshot` directory which, in turn, contains directory trees for each of the snapshots. Each of these directory trees consists of a *frozen* image of the files that were accessible from the export at the time the snapshot was taken (access privileges for these files are preserved intact).
- Similarly, the top-level folder in any CIFS share contains a `~snapshot` folder with similar characteristics. Both with NFS and with CIFS, each directory accessible from the export (share) also contains a hidden `.snapshot (~snapshot)` directory which, in turn, contains *frozen* images of that directory. A global setting can be used to hide `.snapshot` and `~snapshot` from NFS and CIFS clients.

Note: Backing up or copying all files at the root of an NFS export or a CIFS share can have the undesired effect of backing up multiple copies of the directory tree (that is, current file contents plus images preserved by the snapshots; for example, a 10 GB directory tree with four snapshots would take up approximately 50 GB). Administrators can control access to snapshot images by disabling snapshot access for specific NFS exports and CIFS shares. For example, by creating one set of shares for users with snapshots disabled, and a second set of shares with restricted privileges (for administrator access to snapshot images).

2

Using snapshots

Snapshots create near-instantaneous, read-only images of an entire file system at a specific point in time.

- ☐ Managing snapshot rules
- ☐ Creating snapshot rules
- ☐ Modifying snapshot rules
- ☐ Deleting snapshot rules
- ☐ Managing individual snapshots

Managing snapshot rules

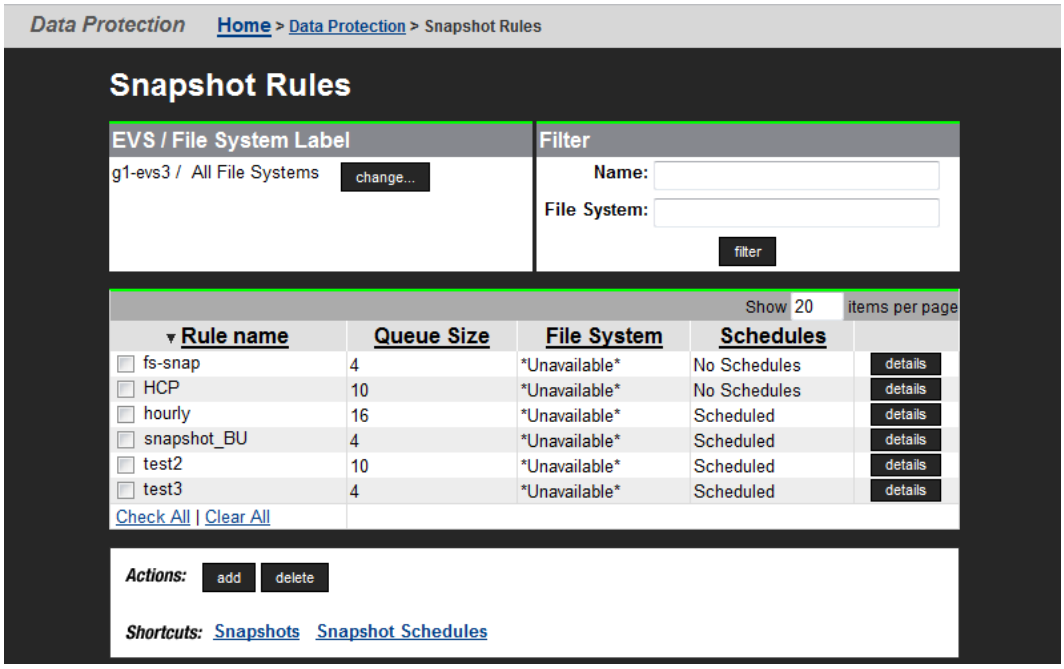
Snapshot rules define scope (that is, what file system), while snapshot schedules define frequency. This section describes how to use Web Manager to create rules and schedules and to assign schedules to rules.

Note: This section does not cover setting up specific storage management applications or tape libraries. Consult the documentation that accompanies the application and tape library for setup instructions.

Creating snapshot rules

Procedure

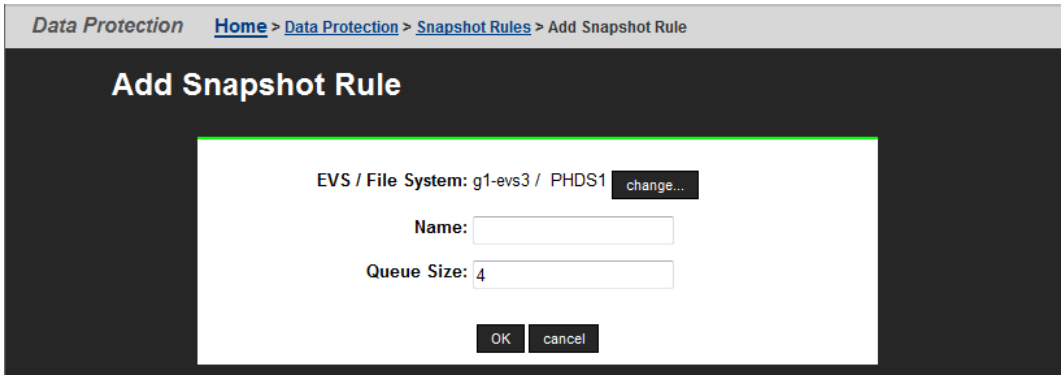
1. Navigate to **Home > Data Protection > Snapshots** to display the **Snapshot Rules** page.



Field/Item	Description
change	Selects the EVS/file system.
Rule name	Rules for the EVS/file system.
Queue Size	Number of snapshots the system keeps before the oldest snapshot is deleted.

Field/Item	Description
File System	The file system for the rule.
Schedule	The schedule for the rule.
details	Opens the **Snapshot Rule Details** page for a rule.
add	Adds a rule.
delete	Deletes a selected rule.
Snapshots	Opens the **Snapshots** page.

2. Click **add** to display the **Add Snapshot Rule** page.



Field/Item	Description
change	Sets the EVS/File system.
Name	The name for the rule.
Queue Size	Number of snapshots to keep before the system automatically deletes the oldest snapshot.
OK	Saves configuration changes, and closes the page.
cancel	Closes the page without saving configuration changes.

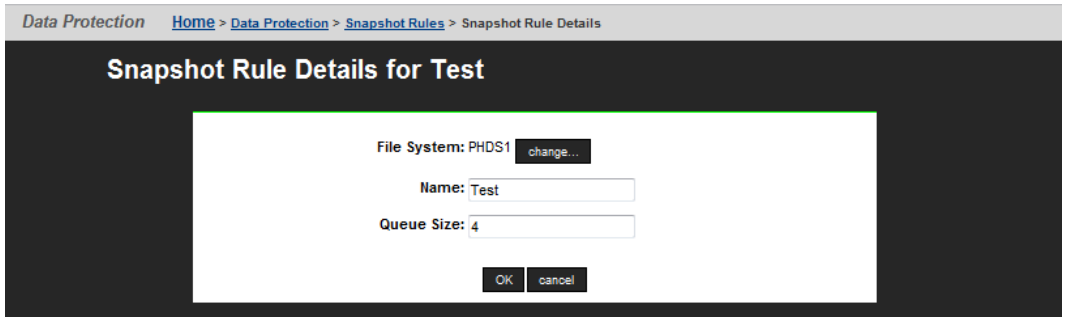
- Click **change** to select the file system.
- In the **Name** field, type a name for the rule (containing up to 30 characters). Do not include spaces or special characters in the name. The name of the rule determines the names of the snapshots that are generated with it. For example, `YYYY-MM-DD_HHMM[timezone information].rulename`. in which date and time are expressed in the indicated format, *timezone information* is a placeholder for the offset from Greenwich Mean Time, and *rulename* is the name of the file. If more than one snapshot is generated per minute by a particular rule, the names will be suffixed with .a, .b, .c and so on. For example, a rule with the name *frequent* generates snapshots called:

```
2002-06-17_1430+0100.frequent
2002-06-17_1430+0100.frequent.a
2002-06-17_1430+0100.frequent.b
```
and so on.

- In the **Queue Size** field, specify the number of snapshots to keep before the system automatically deletes the oldest snapshot. The maximum is 1024 snapshots per rule.

Note: The system automatically deletes the oldest snapshot when the number of snapshots, associated to a snapshot rule, reaches the specified queue limit. However, any or all of the snapshots may be deleted at any time, and new snapshots can be taken.

3. Define the snapshot rule, and select a file system.
4. Assign a schedule.
   a. Select the rule to which you want to add a schedule, and click **details**. Fill the check box next to the name of the rule to which you want to add a schedule, and click **details** to display the **Snapshot Rule Details** page.

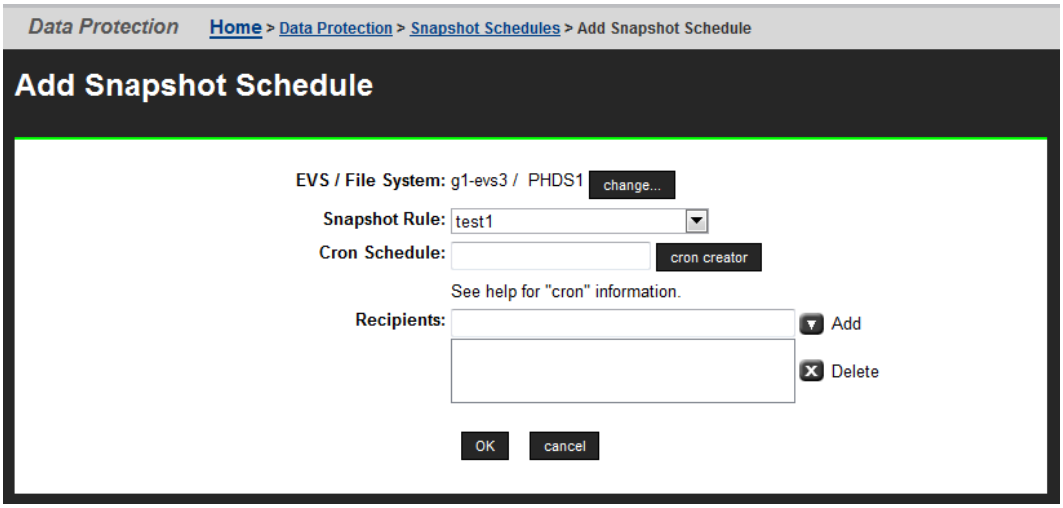


Field/Item	Description
EVS/File System	Displays the EVS and file system.
Name	The name of the snapshot rule. The name can be changed. The name can be up to 10 characters. Do not include spaces or special characters in the name. **Note:** The name of the rule determines the names of the snapshots that are generated with it. For example, a rule with the name **weekly** generates snapshots called **weekly1**, **weekly2**, and so on.

Field/Item	Description
Queue Size	The number of snapshots to keep before the system automatically deletes the oldest snapshot. The maximum is 32 snapshots per rule.
apply	Saves any changes.
Recipients	The **Recipient** consists of one or more email address to whom the system sends an e-mail notification each time it takes a snapshot.
Cron/Schedule	An English explanation of the snapshot schedule or, for more complex schedules, a cron expression of the snapshot schedule. Click **details** to open the **Snapshot Schedule Details** page, in which you can display and modify the selected snapshot schedule.
add	Adds a snapshot schedule for the rule.
delete	Deletes the selected snapshot schedule for the rule.

b. Click **add** to display the **Add Snapshot Schedule** for rule page.

c. Specify the schedule for the rule.



Field/Item	Description
Cron Schedule	Name of the schedule for the rule.
cron creator	Creates a new schedule.
Recipients	One or more email addresses to receive snapshot notifications. Click **Add** to add addresses to the list. Select an address in the list and click **Delete** to remove it. Multiple addresses should be separated with a semicolon (;).
OK	Saves configuration changes, and closes the page.

Field/Item	Description
cancel	Closes the page without saving configuration changes.

You can click **cron creator** and build your schedule, or you can specify the schedule directly in the **Cron Schedule** field.

For more information on the `cron` syntax, refer to the UI help page and the `crontab` command in the *Command Line Reference*.

d. Enter an email address to be notified upon completion of each snapshot.

In the **Recipients** field, you can enter a single email address or multiple email addresses. Multiple addresses should be separated with a semicolon (;). Hitachi Data Systems Support Center recommends sending Snapshot notifications to at least one user.

5. Verify your settings, then click **OK** to save or **Cancel** to decline. You are returned to the **Snapshot Rules** page, which summarizes properties for the rule you just created.

Modifying snapshot rules

Procedure

1. Navigate to **Home > Data Protection > Snapshot Rules**.
2. Modify rule properties:
   a. From the **Snapshot Rules** table, click **details** for a snapshot rule, which opens the **Snapshot Rule Details** page.
   b. As needed, modify the **Name** and **Queue Size** fields, then click apply to save and return to the **Snapshot Rules** page.
3. Modify a rule schedule:
   a. From the **Snapshot Rules** table, click **details** for a snapshot rule, which opens the **Snapshot Rule Details** page.
   b. Click **details** for a snapshot schedule, which opens the **Snapshot Schedule Details** page.
   c. As needed, modify the **Cron Schedule** and **Recipients**.
   d. Click **OK** to save, or **cancel** to decline.

Deleting snapshot rules

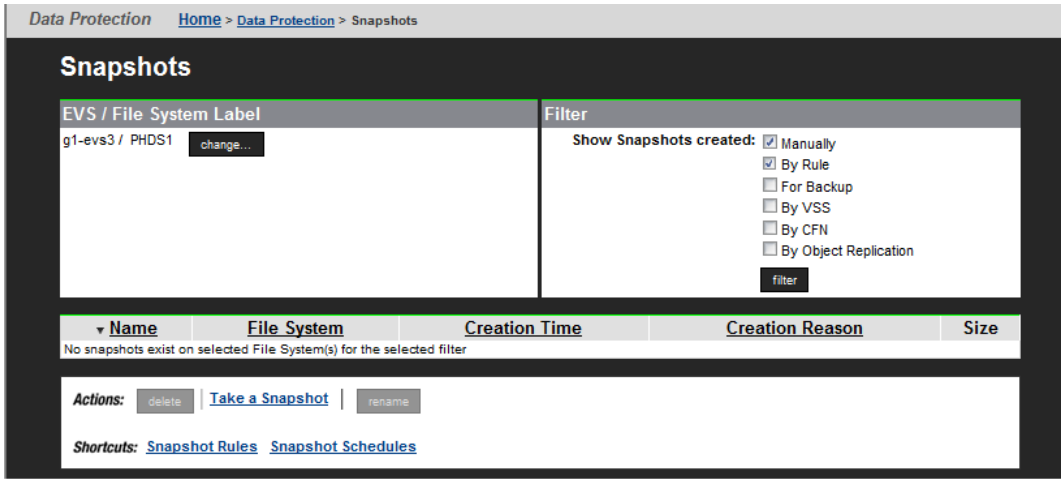
Procedure

1. Navigate to **Home > Data Protection > Snapshot Rules**.
2. From the **Snapshot Rules** table, select a **Snapshot Rule**, and click **delete**.

Managing individual snapshots

Procedure

1. Navigate to **Home > Data Protection > Snapshots** to display the **Snapshots** page.



Field/Item	Description
change	Select a specific file system and display a list of snapshots.
Filter snapshots:	• **Manually** displays snapshots created manually. • **By Rule** displays snapshots created by snapshot rules. • **For Backup** displays snapshots as part of the backup process. • **By VSS** displays snapshots initiated by VSS (the Microsoft Volume Shadow Copy Service). • **By CFN** displays snapshots created by the Changed File Notification feature.
Take a new snapshot	Opens the **Take a snapshot** page.
delete	Removes a selected snapshot.
rename	Enter a new name in the **Rename Snapshot** text field, and then click **rename**.

2. In the **EVS/file system** section, click **change** to select a specific file system and display a list of snapshots.
3. In the filter section, fill the appropriate check boxes to filter the snapshots you want to display, then click **filter**.

   Snapshot filters allow you to limit which snapshots are displayed based on your selection of the reasons or mechanisms that can cause snapshots to be created. Select one or more of the following:

   - **Manually** to display snapshots created manually.

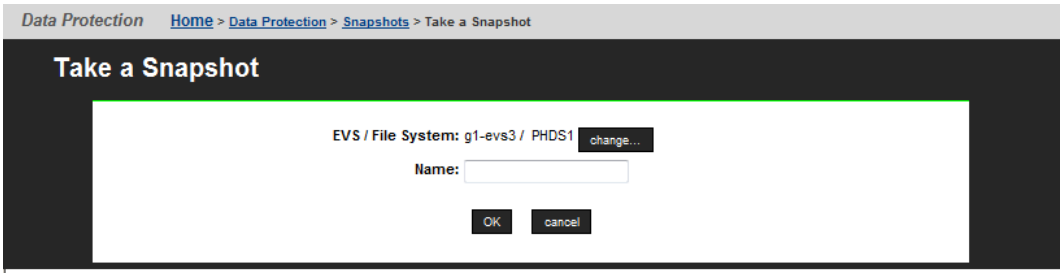
- **By Rule** to display snapshots created by snapshot rules.
- **For Backup** to display snapshots as a part of the backup process.
- **By VSS** to display snapshots initiated by VSS (the Microsoft Volume Shadow Copy Service).
- **By CFN** to display snapshots created by the Changed File Notification feature.

4. Manage the snapshots:

   - Delete an individual snapshot, by selecting it, then clicking **delete**.

Note: Snapshots initiated by the Microsoft Volume Shadow Copy Service (VSS) should be managed through the application that requested the snapshot. You can, however, delete these snapshots through the **Snapshots** page.

   - Delete all the snapshots, by selecting **Check all**, and clicking **delete**.
   - Rename an individual snapshot, by selecting it, entering the new name in the **Rename Snapshot** text field, and clicking **rename**.
   - Take a new snapshot by clicking **Take a Snapshot** to display the **Take a snapshot** page,



Field/Item	Description
change	Select an EVS or file system.
Name	Enter a name for the snapshot (up to 256 characters, no spaces or special characters).
OK	Takes the snapshot.
cancel	Cancels the snapshot

   Enter a **Name** for the snapshot (up to 30 characters, no spaces or special characters). Click **OK** to take the snapshot, or **Cancel** to decline.

Note: Users with permission can also take spontaneous rule-associated snapshot, without waiting for the next scheduled time. This can be done from the command line interface.

3

Managing snapshots initiated by VSS

Snapshots initiated by the Microsoft Volume Shadow Copy Service (VSS) should be managed through the application that requested the snapshot. These snapshots cannot be deleted by rule, but if necessary, you can delete these snapshots through the **Snapshots** page.

Accessing shadow copies initiated by VSS

The VSS Hardware Provider DLL provides support for taking shadow copies initiated by Microsoft's Volume Shadow Copy Service (VSS). The VSS Hardware Provider allows you to take shadow copies of iSCSI LUs located on storage devices managed by NAS servers. VSS shadow copies are exported as iSCSI LUs. After a shadow copy has been taken and exported (or "surfaced"), a pointer is provided to the application that requested the shadow copy. Using this pointer, the application can then access the shadow copy to back up database-type applications such as Microsoft Exchange and SQL Server.

Note: Creating a VSS shadow copy may result in a NAS server snapshot or a FileClone file clone being created on the NAS server.

The VSS Hardware Provider runs on a Windows server (see Installing the VSS Hardware Provider, on page 12). Once installed, the VSS Hardware Provider registers with the Microsoft VSS Service.

When a VSS shadow copy is created, one or more iSCSI LUs are added to the iSCSI target (one iSCSI LU is added for each source LU supplied to VSS). The shadow copy LUs are then visible to the VSS host (the system on which the VSS Hardware Provider is installed) and are used as the backup source.

Note: If a VSS snapshot request contains LUs on different file systems, then only one snapshot will be created for all the LUs in each file system. However, copies of each requested LU are always created and made visible to the VSS host by the NAS server.

Each NAS server or cluster must be configured to allow VSS access.

Removing VSS initiated shadow copies

Snapshots or FileClone file clones created by taking VSS shadow copies should be managed through the application that requested the shadow copy. Shadow copies are either non-persistent or persistent.

For non-persistent shadow copies, once the backup is complete, the shadow copy LUs are removed from the target and any corresponding NAS server snapshots or file clones are deleted.

Persistent shadow copies should be deleted through the backup application whenever possible. Although it is possible to delete a VSS initiated snapshot or FileClone file clone using the CLI or Web Manager, care must be taken to ensure that a backup application is not active and an iSCSI host is not bound

to the shadow copy LUs. Properly deleting a snapshot or file clone will also result in the corresponding shadow copy LUs being removed from the target.

Note: Using the CLI or Web Manager to delete VSS initiated snapshots or file clones, or to remove the shadow copy LUs from their associated iSCSI target, will result in the unexpected removal of a disk from the VSS host system, and can cause the VSS host to crash.

VSS restrictions

- VSS is not supported on iSCSI LUs formatted as dynamic disks, only basic disks are supported.
- Quick Snapshot Restore of iSCSI LUs used by VSS is not supported.
- VSS initiated snapshots may not be backward compatible between major firmware releases. For example, snapshots taken on a NAS server running firmware version SU 6.x cannot be accessed by the VSS host if the NAS server is returned to firmware version SU 5.x. For information on backward compatibility of VSS initiated snapshots between releases, contact your technical support representative.

Configuring the NAS server for VSS shadow copies

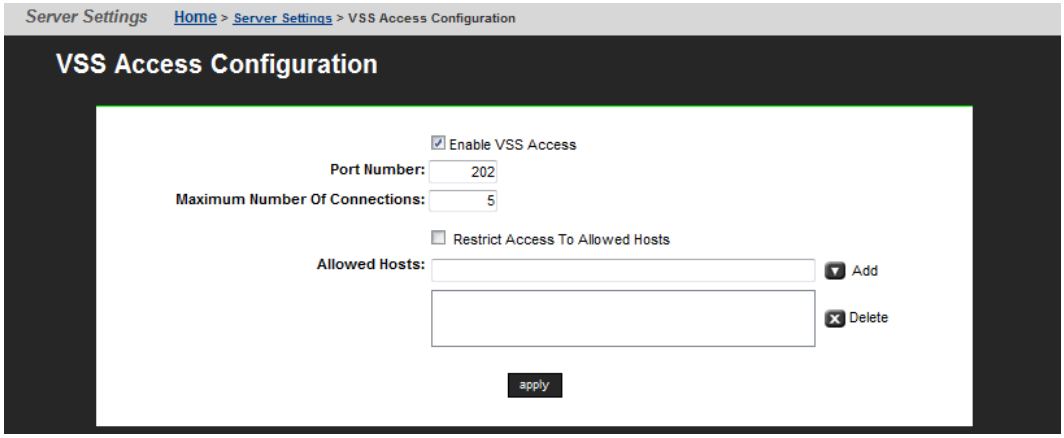
Configuring VSS access to a server

You can configure a storage server to allow VSS access using Web Manager or the CLI command **`mscfg`**.

To configure the storage server using Web Manager:

Procedure

1. Navigate to **Home > Server Settings > VSS Access Configuration** to display the **VSS Access Configuration** page.



2. Enter the required information, as described in the following table:

Table 3-1 VSS Access Configuration

Field/Item	Description
Enable VSS Access	Fill the check box to allow access by the VSS protocol, or empty the checkbox to disable access using that protocol. **Note:** To use VSS you must install and configure the VSS Hardware Provider software.
Port Number	Enter the port number that the storage server should monitor for communication through the protocol. The default is port 202.
Maximum Number Of Connections	Specifies the maximum number of simultaneous connections to the server. You can allow up to five simultaneous connections.
Restrict Access To Allowed Hosts	Fill the check box to restrict protocol access to the hosts specified on this page. Make sure the check box is empty to enable the protocol to access any host.
Allowed Hosts	If protocol access is restricted to specified hosts, use these fields to specify the hosts to which the protocol has access. **Note:** If protocol access is restricted to specified to hosts, make sure the SMU is an allowed host. • Allowed Hosts (field). In the Allowed Hosts field, enter the IP address of a host that the protocol is allowed to access, then click **Add** to insert that host into the list of allowed hosts. **Note:** If the system has been set up to work with a name server, you can identify allowed hosts by IP address or hostname. Wildcard Usage: You can specify an IP address using the * character, such as: `10.168.*.*` or `172.*.*.*`. • Allowed Hosts (list). This list displays the IP address or hostname of each of the hosts that the protocol is allowed to access. To delete a host, select its IP address or hostname from the list and click **Delete**.
Add	Inserts that host into the Allowed Hosts list.
Delete	Deletes the selected host from the Allowed Hosts list.
apply	Saves configuration changes, and closes the page.

Installing the VSS hardware provider

The VSS Hardware Provider software has the following requirements:

- The NAS server: Firmware version 5.1 or later.
- The VSS host:
  - Windows Server 2003 with SP2 or later (32-bit or 64-bit version) or Windows Server 2008 (32-bit or 64-bit version).
  - 16 MB of free disk space.

Installation process

During installation, the installation program automatically installs the correct 32-bit or 64-bit executable for the operating system, and the installation program also installs:

- The Manage NAS Server Connections utility, which allows you to specify each NAS server or cluster that you want to be able to access using VSS. A shortcut is placed in the Start menu for easy access to the utility.
- Microsoft Visual Studio 2005 SP1 Redistributable runtime library, which is used by the VSS Hardware Provider. After installation this library is listed in the **Add or Remove Programs Control Panel** as Microsoft Visual C++ 2005 Redistributable. You can display the version number in the **Control Panel** by highlighting the application, and clicking the Click here for support information link.

On the last dialog of the installation program, select Manage Hitachi NAS Platform/High-performance NAS Platform connections for VSS provider to start the Manage NAS Server Connections utility. Note that you can choose to configure your server connections at a later time, and access the utility through the Start menu (Hitachi NAS Platform VSS Hardware Provider). If you receive a message prompting you to restart your computer to complete the installation, you must reboot before using the Manage NAS Server Connections utility.

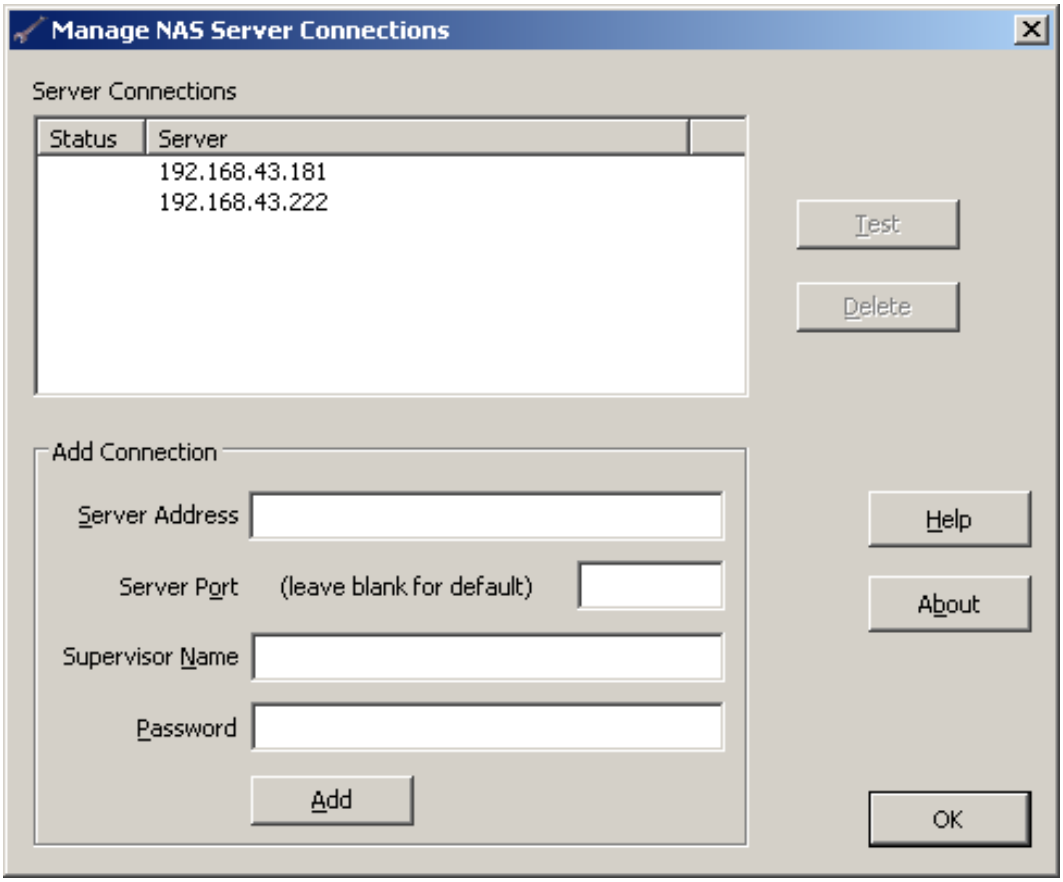
Note: If a previous version of the Hitachi NAS Platform VSS Hardware Provider is already present on the VSS host, we recommend that you uninstall it before installing the new version. To install a new version or uninstall a previous version, there must not be a connection open between the VSS Hardware Provider and the Hitachi NAS Platform. You can uninstall the application through the Windows Start menu.

Configuring NAS server connections

This utility allows you to specify the VSS connection information for each NAS server or cluster. The utility also displays any NAS server connections that have been configured.

Server connections are configured using the Manage NAS Server Connections utility, shown in this section. You can start this utility during the VSS Hardware Provider installation (by selecting Manage Hitachi NAS Platform connections for VSS provider on the last dialog of the installation program) or after installation through the Windows Start menu.

To configure a VSS connection for a NAS server, specify the information in the Add Connection area (Server Address, Server Port, Supervisor Name, and Password) and click Add. This creates a unique VSS credential (discussed in VSS Credentials on page 28), which is saved on the target NAS server and on the VSS host. Once added, the NAS server's IP address or DNS name appears in the Server column of the Server Connections list in this dialog. The Status column lists the status of the VSS credential.



Item/Field	Description
Server Connections	This table lists the DNS name or IP address of all configured NAS servers, along with their status. This table has two columns: Status and Server. The Server column lists the DNS name or IP address of all NAS servers that have had their connection information specified through this utility (that is, NAS servers for which this host has a VSS credential). If a non-default port number was used when the VSS credential was created, then that number is shown following the server's DNS name or IP address. The Status column lists the status of the VSS credential. A status is provided only after the server has been tested (by selecting the server and clicking Test). The possible status values are blank (no test run), OK, or Fail.

Item/Field	Description
	A status of "Fail" indicates that the VSS host cannot connect to the NAS server. If this occurs, make sure your NAS server is running and that you can PING the server. You can also use the mscfg vss and vss-account CLI commands to ensure that VSS is enabled, and that the NAS server's copy of the credential has not been removed.
Server Address	Specify either the IP address or the DNS name of the NAS server or cluster.
Server Port	Leave blank to use the VSS default port (202). If the server has been configured to use a non-default VSS management port, specify that port number.
Supervisor Name	Specify the name of a management account with supervisor privileges on the NAS server. (The supervisor name is not saved by the VSS Hardware Provider.)
Password	Specify the password of the Supervisor Name provided. (The password is not saved by the VSS Hardware Provider.)
Test	Verifies that the selected server and its VSS credential are still valid. The test establishes a connection to the NAS server's "VSS management server" and sends a loopback message to verify functionality. The test returns either OK or Fail, which is displayed in the Status column.
Delete	Removes the selected NAS server's credential. The credential is removed from the VSS host, and, if server connectivity is possible, the credential is also removed from the NAS server.
Help	Displays help information.
About	Displays version information.
Add	After filling in the fields in the Add Connection area, clicking Add creates a unique VSS credential for the NAS server. The credential is saved on the NAS server and on the VSS host (the system running the VSS Hardware Provider).
OK	After adding one or more connections, clicking OK closes the dialog. While entering information in the Add Connection area, clicking OK steps you through the fields, and pressing Escape on the keyboard closes the dialog.

About VSS credentials

A VSS credential is saved on both the VSS host and the NAS server. The server address and port number are saved along with the credential. This means that if the NAS server's VSS management port setting is changed, any existing VSS credentials for that server must be removed and new credentials must be created. If a DNS name is used for a NAS server, then changes to the server's IP address alone will not require removing and recreating the credential.

A VSS credential has limited rights on the server: it can only be used to perform VSS-related operations using the VSS management interface. In particular it cannot be used to gain access to the normal NAS server management console, either locally or remotely.

Hitachi Data Systems

Corporate Headquarters
2845 Lafayette Street
Santa Clara, California 95050-2639
U.S.A.
www.hds.com

Regional Contact Information

Americas
+1 408 970 1000
info@hds.com

Europe, Middle East, and Africa
+44 (0) 1753 618000
info.emea@hds.com

Asia Pacific
+852 3189 7900
hds.marketing.apac@hds.com

Hitachi Data Systems

MK-92USF008-05