

Snapshot Administration Guide

Hitachi Virtual Storage Platform Gx00 and Fx00 with NAS Modules

VSP N series

Hitachi NAS Platform

Release 14.6 or higher

© 2011, 2019 Hitachi, Ltd. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including copying and recording, or stored in a database or retrieval system for commercial purposes without the express written permission of Hitachi, Ltd., or Hitachi Vantara LLC (collectively "Hitachi"). Licensee may make copies of the Materials provided that any such copy is: (i) created as an essential step in utilization of the Software as licensed and is used in no other manner; or (ii) used for archival purposes. Licensee may not make any other copies of the Materials. "Materials" mean text, data, photographs, graphics, audio, video and documents.

Hitachi reserves the right to make changes to this Material at any time without notice and assumes no responsibility for its use. The Materials contain the most current information available at the time of publication.

Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Vantara LLC at https://support.hitachivantara.com/en_us/contact-us.html.

Notice: Hitachi products and services can be ordered only under the terms and conditions of the applicable Hitachi agreements. The use of Hitachi products is governed by the terms of your agreements with Hitachi Vantara LLC.

By using this software, you agree that you are responsible for:

1. Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals; and
2. Verifying that your data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

Notice on Export Controls. The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.

Hitachi and Lumada are trademarks or registered trademarks of Hitachi, Ltd., in the United States and other countries.

AIX, AS/400e, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, FlashCopy, GDPS, HyperSwap, IBM, Lotus, MVS, OS/390, PowerHA, PowerPC, RS/6000, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z14, z15, z16, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

Active Directory, ActiveX, Bing, Excel, Hyper-V, Internet Explorer, the Internet Explorer logo, Microsoft, Microsoft Edge, the Microsoft corporate logo, the Microsoft Edge logo, MS-DOS, Outlook, PowerPoint, SharePoint, Silverlight, SmartScreen, SQL Server, Visual Basic, Visual C++, Visual Studio, Windows, the Windows logo, Windows Azure, Windows PowerShell, Windows Server, the Windows start button, and Windows Vista are registered trademarks or trademarks of Microsoft Corporation. Microsoft product screen shots are reprinted with permission from Microsoft Corporation.

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

Copyright and license information for third-party and open source software used in Hitachi Vantara products can be found in the product documentation, at <https://www.hitachivantara.com/en-us/company/legal.html> or https://knowledge.hitachivantara.com/Documents/Open_Source_Software.

Contents

Preface.....	4
Related Documentation.....	4
Accessing product documentation.....	7
Getting help.....	7
Comments.....	7
Chapter 1: Snapshots.....	8
Latest snapshot.....	8
Accessing snapshots through NFS exports and SMB shares.....	9
Chapter 2: Using snapshots.....	10
Managing snapshot rules.....	10
Creating snapshot rules.....	10
Modifying snapshot rules.....	15
Deleting snapshot rules.....	15
Managing individual snapshots.....	15
Viewing snapshot schedules.....	19
Chapter 3: Managing snapshots initiated by VSS.....	20
Snapshots and the volume shadow copy service (VSS).....	20
Accessing shadow copies initiated by VSS.....	21
Removing VSS initiated shadow copies.....	22
VSS restrictions.....	22
Configuring the NAS server for VSS shadow copies.....	22
Configuring VSS access to a server.....	22
Installing the VSS hardware provider.....	24
Installation process.....	25
Configuring NAS server connections (HNAS server only)	25
About VSS credentials.....	27
Chapter 4: Microsoft file server remote VSS protocol (MS-FSRVP) support.....	28

Preface

This guide provides information about configuring the server to take and manage snapshots. Note that some features apply only to individual platforms and may not be applicable to your configuration.

Virtual Storage Platform G400, G600, G800 and Virtual Storage Platform F400, F600, F800 storage systems can be configured with NAS modules to deliver native NAS functionality in a unified storage platform. The term 'NAS module' in this document also applies to VSP F series, VSP G series, and VSP N series. The unified VSP Gx00 models, VSP Fx00 models, and VSP N series models automatically form a two-node cluster in a single chassis upon installation, with no external cabling required.

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.

Command Line References

The Command Line Reference provides information on the commands used to manage your system, and includes relevant information on the operation of your hardware and software. Depending on the model of your server or cluster node, refer to the Command Line Reference that is appropriate for your system.

- *NAS Module Server Command Line Reference*
- *Command Line Reference for models 4060, 4080, and 4100*
- *Command Line Reference for models 3080, 3090 and 4040*
- *Command Line Reference for models 5200 and 5300*

Administration Guides

- *System Access Guide* (MK-92HNAS014)—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)—Provides information about administering servers, clusters, and server farms. Includes information about licensing, name spaces, upgrading software, monitoring servers and clusters, and backing up and restoring configurations.
- *Storage System User Administration Guide* (MK-92HNAS013)—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)—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)—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) —Provides information about the Data Migrator feature, including how to set up migration policies and schedules.
- *Storage Subsystem Administration Guide* (MK-92HNAS012)—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)—Provides information about configuring the server to take and manage snapshots.
- *Replication and Disaster Recovery Administration Guide* (MK-92HNAS009)—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)—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)—Provides information about configuring the server to work with NDMP, and making and managing NDMP backups.



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 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 and Hitachi Unified Storage Series 4000 Hardware Reference* (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 NAS 5000 Series Hardware Reference* MK-92HNAS089—Provides an overview of the Hitachi NAS Platform Series 5000 server hardware, describes how to resolve any problems, and how to replace potentially faulty components.
- *Hitachi NAS Platform System Manager Unit (SMU) Hardware Reference* (MK-92HNAS065)—This document describes the usage and replacement instructions for the SMU 300/400.

Best Practices

- *Hitachi NAS Platform Best Practices Guide for NFS with VMware vSphere* (MK-92HNAS028)—This document covers best practices specific to using VMware vSphere with the Hitachi NAS platform.
- *Hitachi NAS Platform Deduplication Best Practice* (MK-92HNAS031)—This document provides best practices and guidelines for using 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.
- *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 Data Systems SU 12.x Network File System (NFS) Version 4 Feature Description* (MK-92HNAS056)—This document describes the features of Network File System (NFS) Version 4.
- *Hitachi NAS HDP Best Practices* (MK-92HNAS057)—This document lists frequently asked questions regarding the use of Hitachi Dynamic Provisioning.
- *Hitachi Multi-tenancy Implementation and Best Practice Guide* (MK-92HNAS059)—This document details the best practices for configuring and using Multi-Tenancy and related features, and EVS security.
- *Hitachi NAS Platform HDP Best Practices* (MK-92HNAS063)—This document details the best practices for configuring and using storage pools, related features, and Hitachi Dynamic Provisioning (HDP).

- *Hitachi NAS Platform System Manager Unit (SMU) Hardware Reference* (MK-92HNAS065)—This document describes the usage and replacement instructions for the SMU 300/400.
- *NAS Platform ICC with Cisco Nexus Reference Guide* (MK-92HNAS085)—This document describes how to configure Cisco Nexus series switches for use as an ICC (intra-cluster communication) switch.
- *File System Snapshots Operational Best Practice* (MK-92HNAS068)—This document provides operational guidance on file system snapshots.
- *Virtual Infrastructure Integrator for Hitachi Storage Platforms Operational Best Practice* (MK-92HNAS069)—This document provides operational guidance on Hitachi Virtual Infrastructure Integrator for the HNAS platform.
- *Hitachi NAS Platform Replication Best Practices Guide* (MK-92HNAS070)—This document details the best practices for configuring and using HNAS Replication and related features.
- *Hitachi NAS Platform to Hitachi Virtual Storage Platform Unified Gx00 Models Migration Guide* (MK-92HNAS075)—This best practice guide describes how to perform a data-in-place migration of the Hitachi NAS Platform and Virtual Storage Platform (VSP) Gx00 File solution to the VSP Gx00 platform.

Accessing product documentation

Product user documentation is available on the Hitachi Vantara Support Website: <https://knowledge.hitachivantara.com/Documents>. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Getting help

The [Hitachi Vantara Support Website](#) is the destination for technical support of products and solutions sold by Hitachi Vantara. To contact technical support, log on to the Hitachi Vantara Support Website for contact information: https://support.hitachivantara.com/en_us/contact-us.html.

[Hitachi Vantara Community](#) is a global online community for Hitachi Vantara customers, partners, independent software vendors, employees, and prospects. It is the destination to get answers, discover insights, and make connections. **Join the conversation today!** Go to community.hitachivantara.com, register, and complete your profile.

Comments

Please send comments to doc.comments@hitachivantara.com. Include the document title and number, including the revision level (for example, -07), and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara LLC.

Thank you!

Chapter 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 allow 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 don't consume any disk space when they are created. 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 SMB, NFS, FTP, or NDMP.



Note: Snapshots alone should not be considered a backup solution, as they do not provide a second copy of data in a different location.

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 SMB 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.

Accessing snapshots through NFS exports and SMB shares

NFS exports and SMB shares can easily access snapshots, so that users can restore older versions file systems.

- 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 file systems 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 SMB share contains a `~snapshot` folder with similar characteristics. Both with NFS and with SMB, 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 SMB clients.



Note: Backing up or copying all files at the root of an NFS export or an SMB 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 SMB 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).

Chapter 2: Using snapshots

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

Managing snapshot rules

Snapshot rules define scope (that is, what file system), while snapshot schedules define frequency. This section describes how to use NAS 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 > Snapshot Rules** to display the **Snapshot Rules** page.

Rule name	Queue Size	File System	Schedules	
fs-snap	4	*Unavailable*	No Schedules	details
HCP	10	*Unavailable*	No Schedules	details
hourly	16	*Unavailable*	Scheduled	details
snapshot_BU	4	*Unavailable*	Scheduled	details
test2	10	*Unavailable*	Scheduled	details
test3	4	*Unavailable*	Scheduled	details

Field/Item	Description
EVS / File System Label	The name of the EVS and file system.
change	Enables you to select a different EVS/file system.
Filter	<p>Rule 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.</p> <p>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, etc...</p> <p>File System: The current file system for the snapshot. Click filter to filter snapshots created by snapshot rules.</p>
Rule name	The name of the rule for the EVS/file system.
Queue Size	Number of snapshots the system keeps before the oldest snapshot is deleted.
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.
Snapshot Schedules	Opens the Snapshots Schedules page.

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

Data Protection [Home](#) > [Data Protection](#) > [Snapshot Rules](#) > Add Snapshot Rule

Add Snapshot Rule

EVS / File System: g1-evs3 / PHDS1 [change...](#)

Name:

Queue Size: 4

OK **cancel**

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. The default queue size is four. The maximum size is 1024.

- 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 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.

Data Protection Home > Data Protection > Snapshot Rules > Snapshot Rule Details

Snapshot Rule Details for Test

File System: PHDS1

Name:

Queue Size:

Field/Item	Description
File System	Displays the current file system. Click change to select a different file system.
Name	The name of the snapshot rule. The name can be changed. Do not include spaces or special characters in the name. Asterisks can be used as a wildcard for zero or more characters, and are used for a case-insensitive substring match. 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.
Queue Size	The number of snapshots to keep before the system automatically deletes the oldest snapshot. The maximum is 1024.

- b. Click **add** to display the **Add Snapshot Schedule** for rule page.
- c. Specify the schedule for the rule.

Data Protection Home > Data Protection > Snapshot Schedules > Add Snapshot Schedule

Add Snapshot Schedule

EVS / File System: g1-evs3 / PHDS1

Snapshot Rule:

Cron Schedule:

See help for "cron" information.

Recipients:

Field/Item	Description
EVS/File System	Displays the name of the currently selected EVS and file system. Click change to select a different file system.
Snapshot Rule	List of possible snapshot rules to select from.
Cron Schedule	<p>Displays the schedule in crontab syntax. If you are familiar with the Unix crontab format, you can enter the schedule directly in the field. Otherwise, click cron creator to open the Build Cron Expression dialog and configure to schedule.</p> <p><i>Cron expression syntax:</i> The cron expression is a series of five numbers that indicate the snapshot schedule. The syntax is <i>mm hh dd yy z</i>, in which <i>mm</i> is the minutes (0-59), <i>hh</i> is the hour (0-23), <i>dd</i> is the day of the month (1-31), <i>yy</i> is the month (1-12), and <i>z</i> is the day of the week (0-6, Sunday is 0 or 7). For example: 15 2 21 3 * takes a snapshot at 2:15 AM on the 21st of March, and 5 15 * * 6 takes a snapshot at 3:05 PM every Saturday.</p>
cron creator	Creates a new schedule.
Recipients	One or more email addresses to receive snapshot notifications. To add an address in the list, enter the address and click Add . To remove an address, select it in the list and click Delete .

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 Vantara 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**.



Caution: When a snapshot rule is deleted, the snapshots and snapshot schedules associated with the rule will also be deleted.

Managing individual snapshots

Procedure

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

Situations

EVS / File System Label		Filter		
g5-evs1 / All File Systems	change...	Show Snapshots created: Manually, By Rule filter...		
Show 20 Items per page Name File System Creation Time Creation Reason Freeable Space				
<input type="checkbox"/> 2015-10-19_1200-0700.test g5-fs1 2015-10-19 12:00:00 (PDT) By Rule 58.25 MB Refresh Size <input type="checkbox"/> 2015-10-26_1200-0700.test g5-fs1 2015-10-26 12:00:00 (PDT) By Rule 53.81 MB Refresh Size <input type="checkbox"/> 2015-11-02_1200-0800.test g5-fs1 2015-11-02 12:00:00 (PST) By Rule Show Size <input type="checkbox"/> 2015-11-09_1200-0800.test g5-fs1 2015-11-09 12:00:00 (PST) By Rule Show Size				
Check All Clear All				
Actions: delete Take a Snapshot Rename Snapshot: <input type="text"/> rename Shortcuts: Snapshot Rules Snapshot Schedules				

[Home](#) | [About](#) | [Sign Out](#)

Field/Item	Description
EVS / File system Label	Displays the current source EVS or file system for the snapshot.
change	Enables you to selects a different EVS or file system.
Filter	<p>Filters the snapshot list. The following creation reasons are available:</p> <ul style="list-style-type: none"> ▪ Manually displays snapshots created manually. ▪ By Rule displays snapshots created by snapshot rules. ▪ For Backup and File-based Replication displays snapshots as part of the backup process. ▪ By Volume Shadow Copy Service displays snapshots initiated by VSS. ▪ By Object Replication displays snapshots created by the Object Replication feature. ▪ By Application displays snapshots created by API applications. <p>You can also filter by a specific snapshot name and/or a date creation range.</p>

Field/Item	Description
	<p> Note: Any snapshots created for reasons other than those in the categories above are not listed in NAS Manager. To view these snapshots, use the snapshot-list CLI command.</p>
Name	The name of the snapshot. The name can be up to 255 characters and cannot include any spaces or special characters except for asterisks which can be used as wildcards to match any characters.
File system	The source file system for the snapshot.
Creation Time	The time and date the snapshot was created.
Creation reason	Displays the snapshot creation method. You can create snapshots by using the methods described in the Filter field.
Freeable Space	Click Show size to display the amount of disk space released when the snapshot is deleted (this is supported only on file systems that use block-based snapshots). Click Refresh size to update the value.
Take a snapshot	Opens the Take a snapshot page in which you can create a snapshot manually.
delete	Removes a selected snapshot.
rename	Enter a new name in the Rename Snapshot text field, and then click rename . Note that you can only rename snapshots that are created manually and not those created By Rule.
Snapshot Rules	Opens the Snapshot Rules page. To schedule snapshots, you must first create a rule.
Snapshot Schedules	Opens the Snapshot Schedules page in which you can set a time schedule for creating snapshots.

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, select the appropriate check boxes to filter the snapshots that you want to display, and 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).
4. Manage the snapshots:
- Delete an individual snapshot by selecting it, and 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 in the **Snapshots** page.

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

The following table describes the fields on this page:

Field/Item	Description
change	Select an EVS or file system.
Name	The name of the snapshot. The name can be up to 255 characters and cannot include any spaces or special characters.
OK	Takes the snapshot.

Enter a name for the snapshot (up to 30 characters with no spaces or special characters). Click **OK** to take the snapshot.



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.

Viewing snapshot schedules

Procedure

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

The following table describes the fields on this page:

Field/Item	Description
EVS/File System Label	Displays the current source EVS or file system for the snapshot. Click change in order to select a different EVS or file system.
Filter	<p>Rule 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.</p> <p> 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.</p> <p>File System: The current file system for the snapshot. Click filter to filter snapshots created by snapshot rules.</p>
Cron/Schedule	An English explanation of the snapshot schedule or, for more complex schedules, a cron expression of the snapshot schedule.
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.
Rule	The name of the snapshot rule.
File System	The current file system for the snapshot.
add	Adds a snapshot schedule for the rule.
delete	Deletes the selected snapshot schedule for the rule.
Snapshots	Opens the Snapshots page.
Snapshot Rules	Opens the Snapshot Rules page. To schedule snapshots, the Admin must first create a rule.

Chapter 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.

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 NAS 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 NAS 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.

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 NAS 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 NAS 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.
- 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 NAS Manager or the CLI command `mscfg`.

To configure the storage server using NAS Manager:

Procedure

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

The screenshot shows the 'VSS Access Configuration' page. At the top, there's a breadcrumb navigation: 'Server Settings' > 'Home' > 'Server Settings' > 'VSS Access Configuration'. The main area has a title 'VSS Access Configuration'. It contains the following fields:

- Enable VSS Access
- Port Number: 202
- Maximum Number Of Connections: 5
- Restrict Access To Allowed Hosts
- Allowed Hosts: (empty input field) with 'Add' and 'Delete' buttons.

At the bottom is a 'apply' button.

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

Field/Item	Description
Enable VSS Access	Select the check box to allow access by the VSS protocol, or clear the check box 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. Note: The port number is not configurable on a NAS module.
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.

Field/Item	Description
	<p>Note: If protocol access is restricted to specified hosts, make sure the SMU is an allowed host.</p> <ul style="list-style-type: none"> ▪ 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. <p>Note: If the system has been set up to work with a name server, you can identify allowed hosts by IP address or hostname.</p> <p>Wildcard Usage: You can specify an IP address using the * character, such as: 10.168.*.* or 172.*.*.*.</p> <ul style="list-style-type: none"> ▪ Allowed Hosts (list). This list displays the IP address or hostname of each of the hosts that the protocol is allowed to access. <p>To delete a host, select its IP address or hostname from the list and click Delete.</p>
Add	Inserts that host into the Allowed Hosts list.
Delete	Deletes the selected host from the Allowed Hosts list.
apply	Saves configuration changes.

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. If you choose to configure your server connections at a later time, access the utility through the Start menu (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.



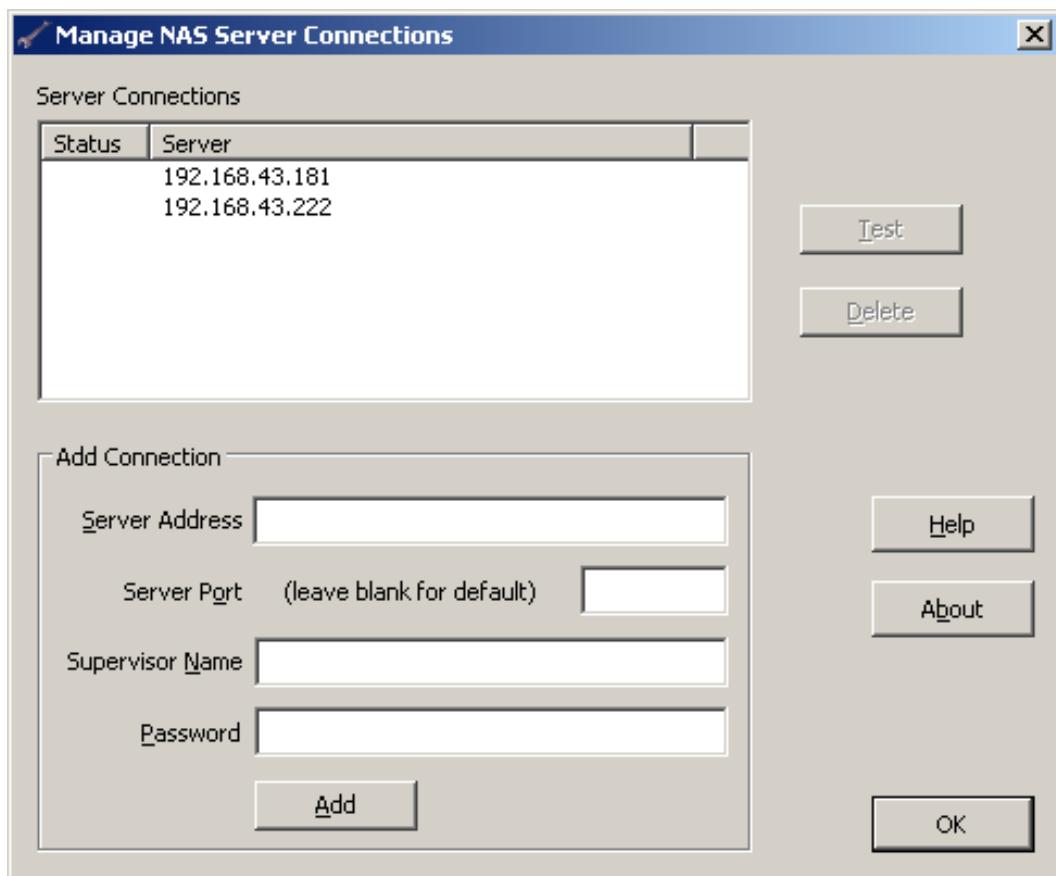
Note: If a previous version of the NAS Platform VSS Hardware Provider is already present on the VSS host, we recommend that you uninstall it before installing the new version. Before installing a new version or uninstalling a previous version, be sure there are no active connections open between the VSS Hardware Provider and the NAS Platform. You can uninstall the application through the Windows Start menu.

Configuring NAS server connections (HNAS server only)

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 \(on page 27\)](#)), 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	<p>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.</p> <p>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.</p> <p>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.</p> <p>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 msfcfg 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.</p>
Server Address	Specify either the IP address or the DNS name of the NAS server or cluster.

Item/Field	Description
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.

Chapter 4: Microsoft file server remote VSS protocol (MS-FSRVP) support

The Microsoft file server remote VSS protocol (MS-FSRVP) allows a file server client to use a shadow copy-aware utility (like the Microsoft DiskShadow utility) to create a point-in-time copy of one or more SMB shares hosted on a NAS server (a shadow copy set). A shadow copy-aware backup utility can use the shadow copy to back up the state of an application that hosts its data on a NAS server. If necessary, the shadow copy can later be used to restore the application state.

Internally, the NAS server uses file cloning to produce the shadow copies. Because it may take some time to produce a copy, the MS-FSRVP protocol is generally used to copy a share containing a small number of large files (less than 10,000) rather than a large number of small files. Shares used to host virtual machine configuration files and disks are often backed up using the MS-FSRVP protocol.

In order to use the Microsoft file server remote VSS protocol to back up a group of SMB shares, you must ensure that:

- The client connecting to the NAS server and the NAS server EVS hosting the share must have SMB3 support enabled. SMB3 support is enabled on a per-EVS basis on the NAS server. To find out the maximum SMB version is supported by a particular EVS, use the **cifs-max-supported-version** command.
- The path of the share to be backed up may not be just the root path of the share (\); the path of the share to be backed up must include a named path (something like \anything). You can use the command **cifs-share list** to display the path of a share.
- The share to be part of a shadow copy set must have at least one plain file or directory under the path root.
- The share to be part of a shadow copy set must contain only directories and plain files. The share must not contain files with hard links, external cross-volume links (XVLs), or files that have been migrated, ingested, or virtualized.

You can use the commands **virtualization-path-list** and **migration-list-paths** to check for migration and virtualization paths.

- By default, the total number of files and directories of a shadow copy set to be committed must be 10000 or less. You can change this maximum using the NAS server **set fsrvp_maxcloneable** command.
- The user issuing the FSRVP protocol request must be a member of the NAS server's local "Backup Operators" group.

The DiskShadow utility typically uses the machine account name to connect to the NAS server when using the FSRVP protocol. Therefore, the machine account of the client must be added to the NAS server's "localgroup," and the machine account name must end with a \$ character. To list and add accounts to the Backup Operators group, use the NAS server command **localgroup**.

- No share in a shadow copy set may include a subdirectory that is mapped to another share (an overlaying path).

To check for overlaying paths, use the NAS server command **cifs-share list** to examine all the shares.

- A share should not be actively in use when a VSS snapshot is taken. We recommend that the clients using the share should be quiesced before the snapshot is taken.

A NAS server administrator can exclude a share from a shadow copy set by using the **cifs-share mod --shadow-copy-use disable <share_name>** command to disallow the share from being in a shadow copy set.



Note: See the *Command Line Reference* for more information on NAS server commands.

Hitachi Vantara

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA

HitachiVantara.com/contact

